

The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors including yellow, orange, red, and various shades of blue and green. Overlaid on this are several large, semi-transparent, wavy shapes in similar color tones, giving the overall image a sense of motion and energy.

cisco *Live!*

Let's go

#CiscoLive



The bridge to possible

Design and Implement Virtual Firewalls

On-premise or in Public Cloud

Jeroen Wittock
TME Technical Leader
BRKSEC-2130



#CiscoLive



Cisco Webex App

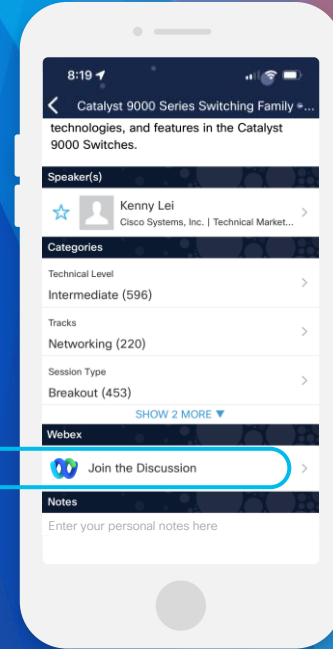
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 9, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2130>

Scope of this Session.

What is this session NOT about?

- Features: EVE, IPS, anti-malware, ...
- How to configure & troubleshoot

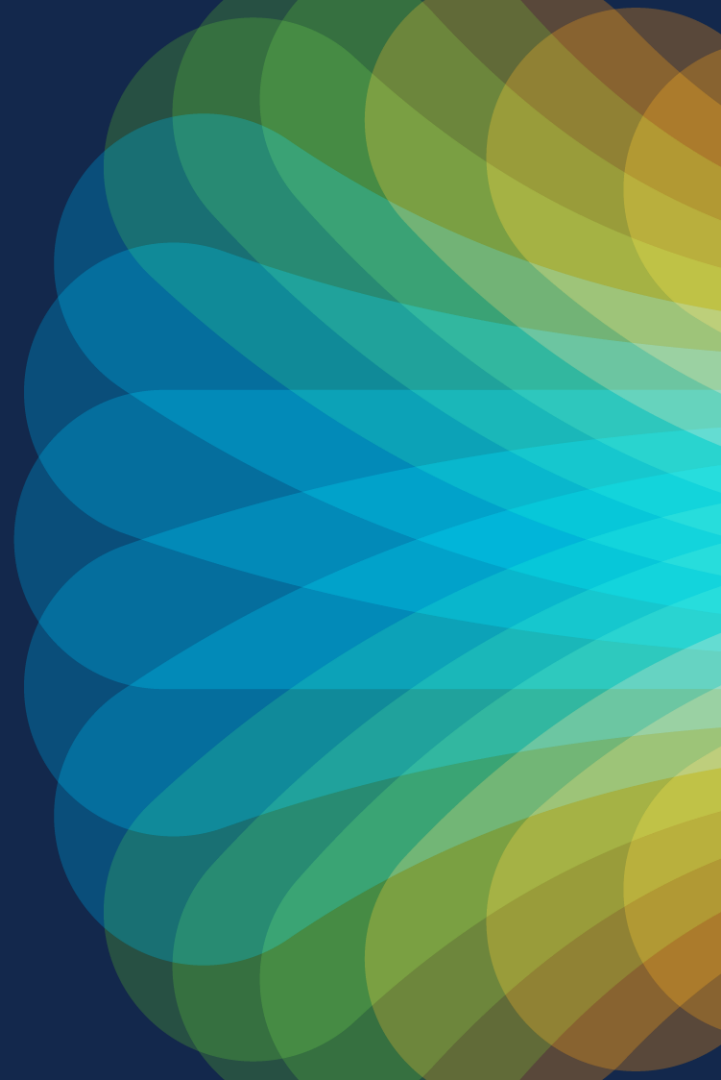
We WILL cover the following:

- Design & Architecture
- Automation

Agenda

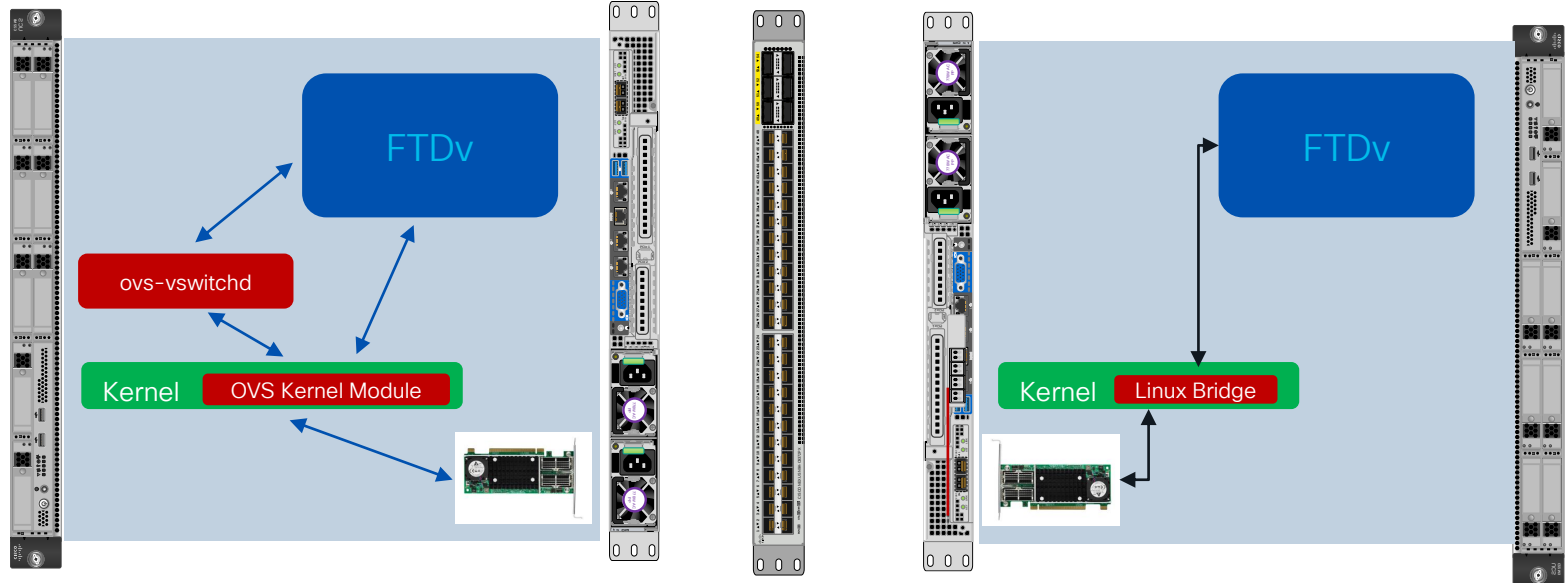
- Networking in Private vs Public Cloud
- Firewall Management Options
- Designs for Private Cloud
- Designs for Public Cloud
- Infrastructure as Code

Networking in Private versus Public Cloud

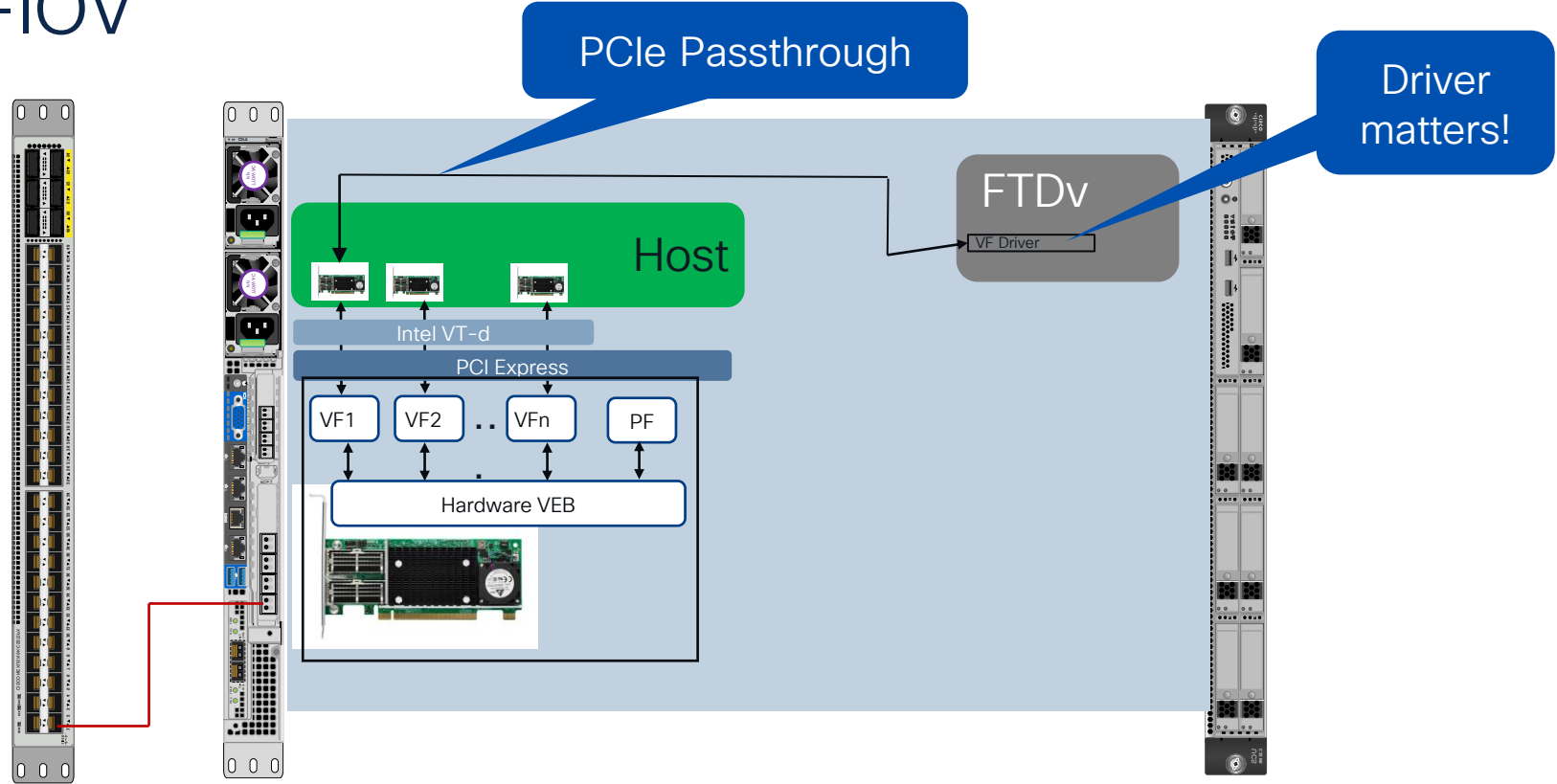


Private Cloud Networking

- Vmware: standard switch, distributed switch, SR-IOV, 3rd party, ..
- KVM: linux bridge, OVS, DPDK & Friends, VPP, SR-IOV, ...



SR-IOV



Public Cloud Networking

Restrictions:

L2 Multicast
L2 Broadcast
GRE
MTU



Consequences:

Routing Protocols
HSRP & VRRP
BFD
GLBP
L2TPv3
802.1q VLAN tagging
AppNav
WCCP

Security Group (SG)

- A *security group* acts as a virtual firewall for your EC2 instances to control incoming and outgoing traffic **to your instance**.
- When you launch an instance, you can specify one or more security groups. If you don't specify a security group, Amazon EC2 uses the default security group.
- Stateful

Or use Cisco NGFW for consistent policies across clouds and additional capabilities.

Security group



Instance

Security Group (SG)

- A *security group* acts as a virtual firewall for your EC2 instances to control incoming and outgoing traffic **to your instance**.
- When you launch an instance, you can specify one or more security groups. If you don't specify a security group, Amazon EC2 uses the default security group.
- Stateful

Or use Cisco NGFW for consistent policies across clouds and additional capabilities.

Security group



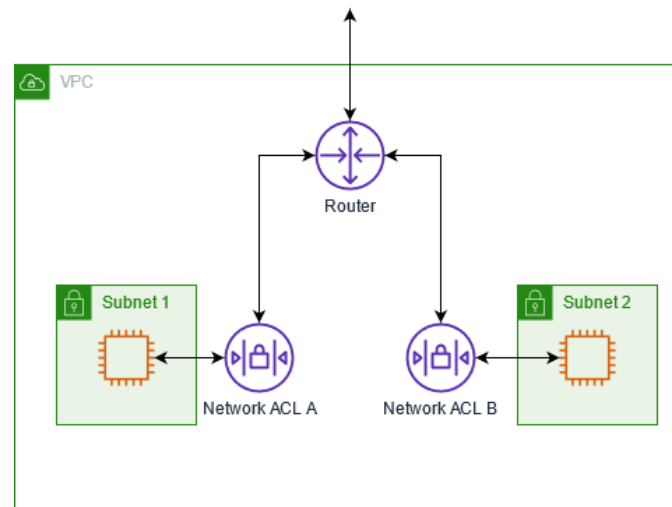
Instance

However NGFW placement would be at subnet level, not host level.

Network ACL (NACL)

- A *network access control list (ACL)* allows or denies specific inbound or outbound traffic **at the subnet level**.
- Stateless

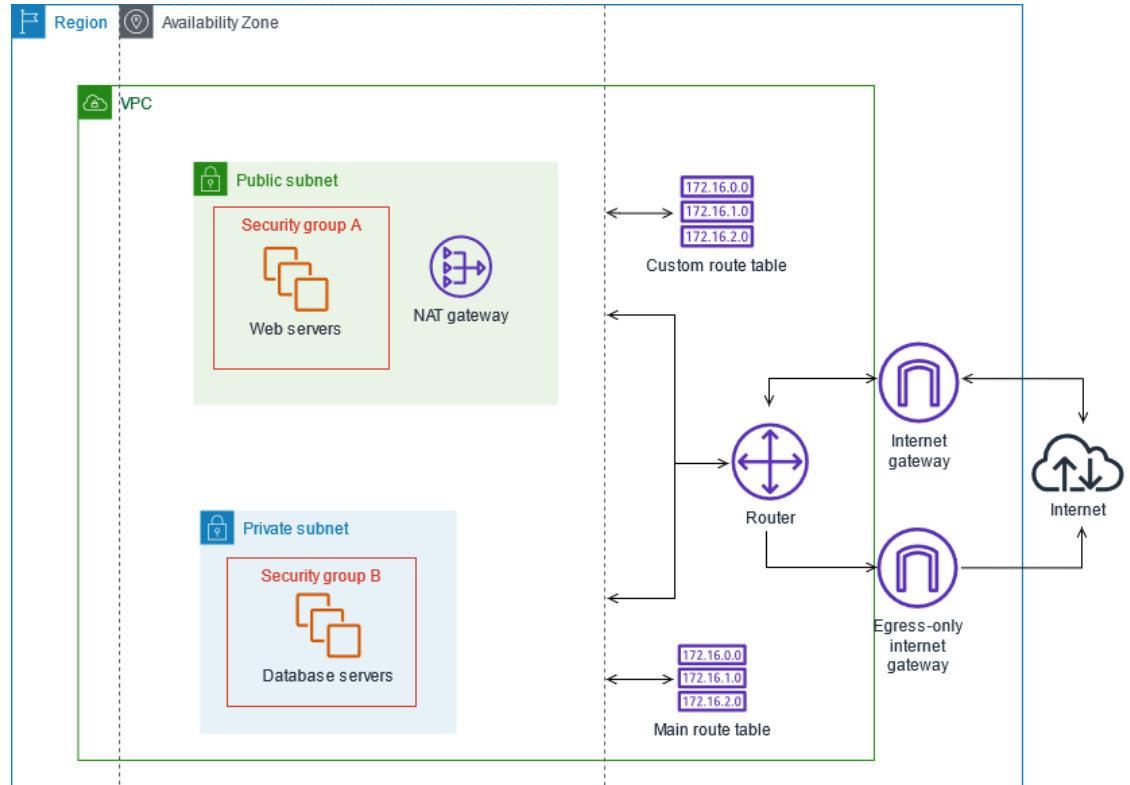
Or use Cisco NGFW for consistent policies across clouds and additional capabilities.



NAT Gateway

- NAT Gateway is deployed in the Public Subnet
- Route Table for private subnet points to NAT GW for outbound traffic
- Egress traffic only

Or use Cisco NGFW for consistent NAT policies across clouds and additional capabilities



Our firewall has Comprehensive Capabilities

Superior Threat Protection

Cisco Talos Security Intelligence



Application
Control, Custom
App Detectors



Intrusion
Prevention



Automation,
Remediation,
and Integration



Malware
Protection and
Sandboxing



URL Filtering and
Categorization



WAN
Capabilities



Firewall,
Routing, NAT



High Availability
and Scalability

010110
110010
001011

VPN/ZTNA



TLS Decryption



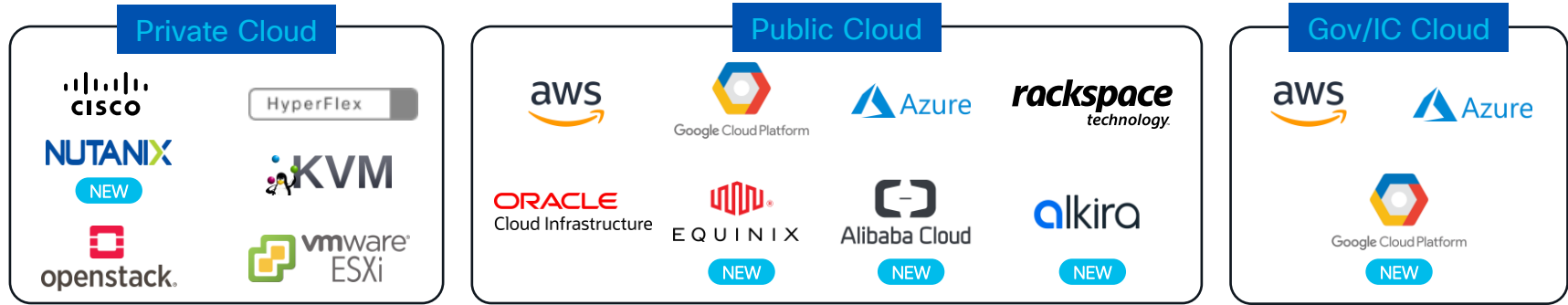
ML-Driven
Encrypted
Visibility Engine



Identity and
Attribute Based
Access Control

Configuration and Analytics Console

Simplifying Firewalling for Multi-cloud



Virtual firewall performance-based licensing from 100Mbps up to 16Gbps

Cloud Leadership

Clustering and Auto Scaling

Integration with cloud native services and infrastructure

Accelerated Networking

Smart & Tiered Licensing

Dynamic Policy

Quick starts, Infrastructure as Code and Automation

Gateway Load balancer integration

Snapshots

Cost

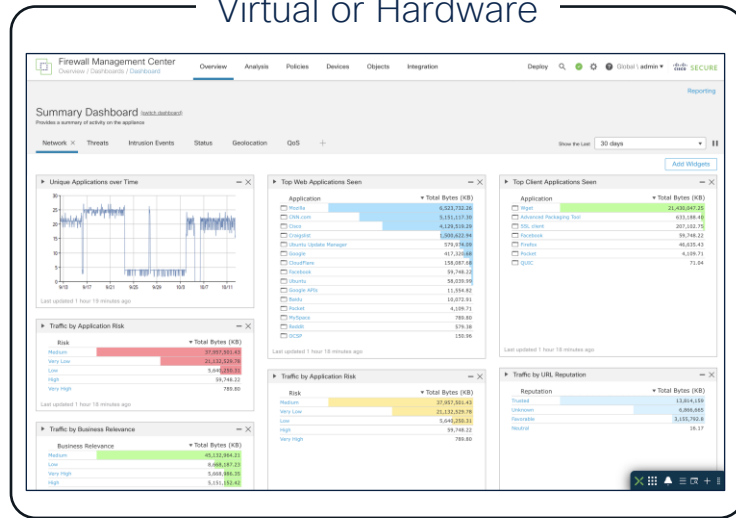
- Infrastructure:
 - private all up front, but very predictable
 - Public: only pay for what you use, when you use. Can become hard to predict, depends on a lot of variables.
- Licensing: PAYG (public cloud only) versus BYOL
- Auto Scale
- Different regions have different cost & different feature availability.

Management Options

Firewall Management Center options

Flexibility of cloud or on-premises options

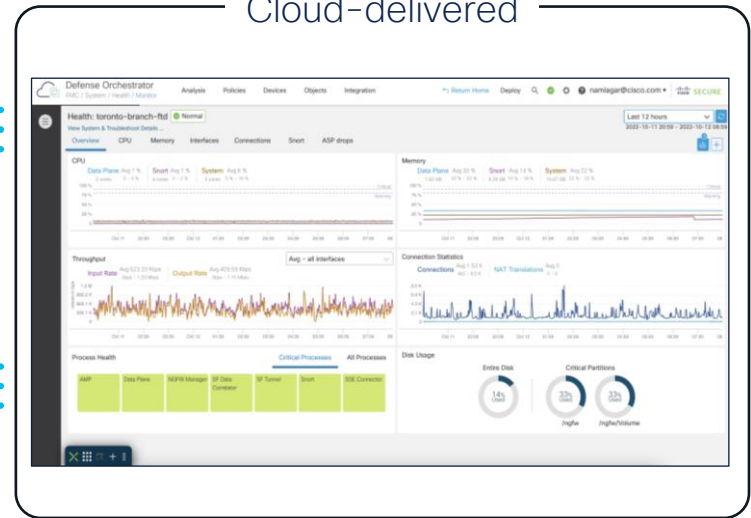
Virtual or Hardware



Firewall
Management
Center



Cloud-delivered



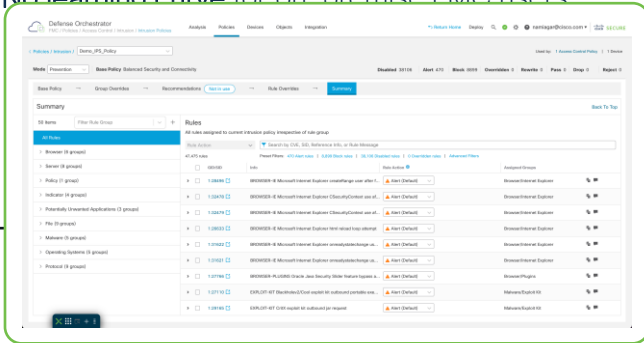
Cisco Secure Firewall Threat Defense Virtual

Cloud-delivered Firewall Management Center (cdFMC)

Cloud-delivered Firewall Management Center works with CDO

Key benefits

- ▶ Eliminate **change management** and **update** overhead
- ▶ No **rack space** and **utility bill**, lowering **operational cost**
- ▶ Cisco ensures **uptime**, increasing **resiliency**
- ▶ **No learning curve** for **on-premise FMC users**

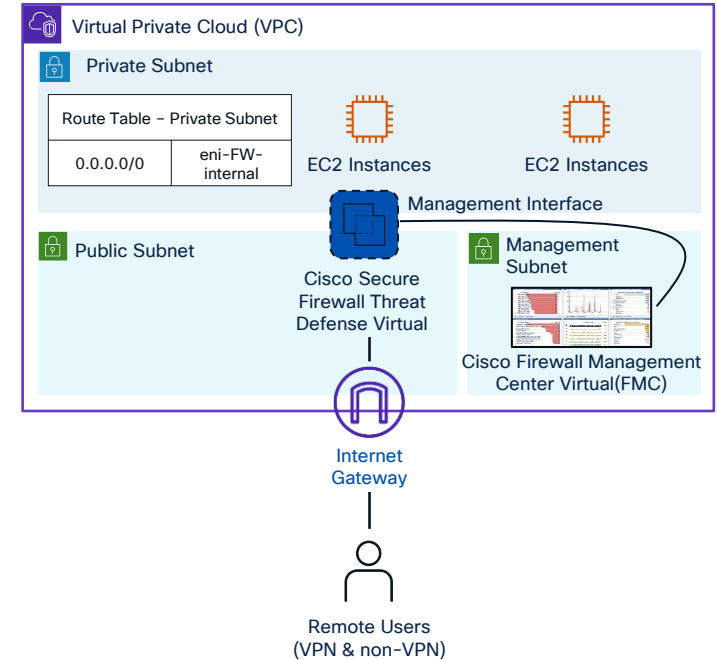


Key features

- ▶ Hybrid management support
- ▶ Support up to **1000 devices**
- ▶ Periodic configuration **snapshots**
- ▶ Easy **migration** from on-premises FMC to cdFMC
- ▶ Real-time security policy updates for multi-cloud environments
- ▶ Secure SaaS applications like O365 using **real-time community feeds**
- ▶ Flexibility between **hybrid and cloud eventing**

Firewall Management Options & Connectivity

- Cisco Secure Firewall can be managed using these options:
 - Firewall Management Center (Centralized Manager)
 - Cloud-delivered Firewall Management Center (Cloud-based)
 - Firewall Device Manager (on-box manager)
 - API
 - Terraform and Ansible
- Connectivity & Management
 - Cisco Firewall Management Center Virtual is available on marketplace.
 - Cisco FMCv can be deployed in the same VPC
 - FMCv requires connectivity to each Secure Firewall on the following ports:
 - TCP 443 (HTTPS UI)
 - TCP 8305 (Sftunnel)



Cisco Firewall Management Center Virtual deployed in the same VPC

Designing in Private Cloud

VMware Feature Support

Table 1. VMware Feature Support for the Threat Defense Virtual

Feature	Description	Support (Yes/No)	Comment
Cold Clone	The VM is powered off during cloning.	No	-
vMotion	Used for live migration of VMs.	Yes	Use shared storage. See vMotion Support .
Hot add	The VM is running during an addition.	No	-
Hot clone	The VM is running during cloning.	No	-
Hot removal	The VM is running during removal.	No	-
Snapshot	The VM freezes for a few seconds.	No	Risk of out-of-sync situations between the management center and managed devices.
Suspend and resume	The VM is suspended, then resumed.	Yes	-
vCloud Director	Allows automatic deployment of VMs.	No	-
VMware FT	Used for HA on VMs.	No	Use the failover feature for threat defense virtual VM failovers.
VMware HA with VM heartbeats	Used for VM failures.	No	Use the failover feature for threat defense virtual VM failovers.
VMware vSphere Standalone Windows Client	Used to deploy VMs.	Yes	-
VMware vSphere Web Client	Used to deploy VMs.	Yes	-

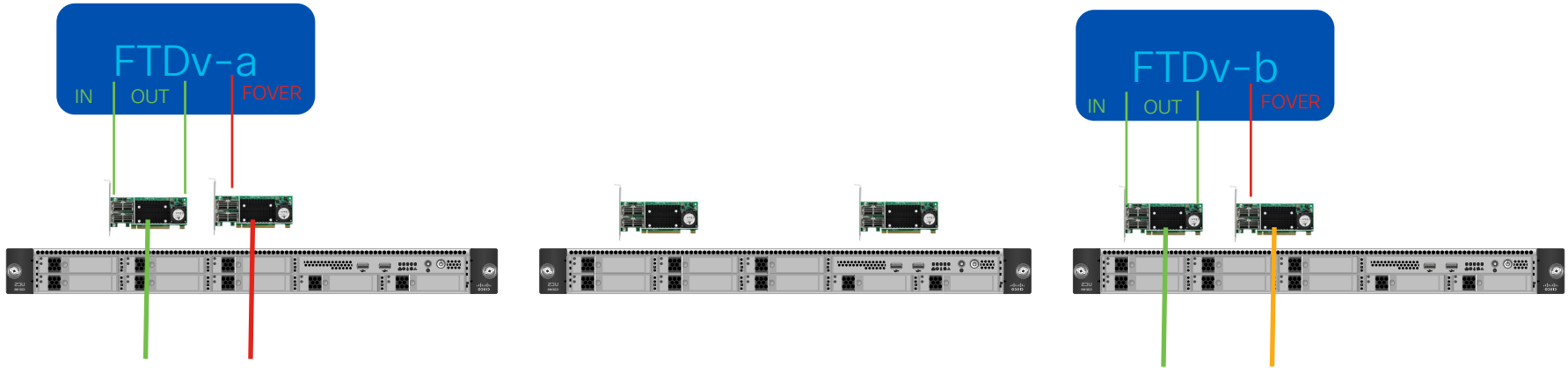
For running FTDv only, there is a procedure to prepare an FTDv for snapshot

Take care when using SRIOV

Is supported for FMCv

High Availability

- Reasonably simple as Failover works.
- Consider anti-affinity.
- Consider dedicated physical links for failover link.

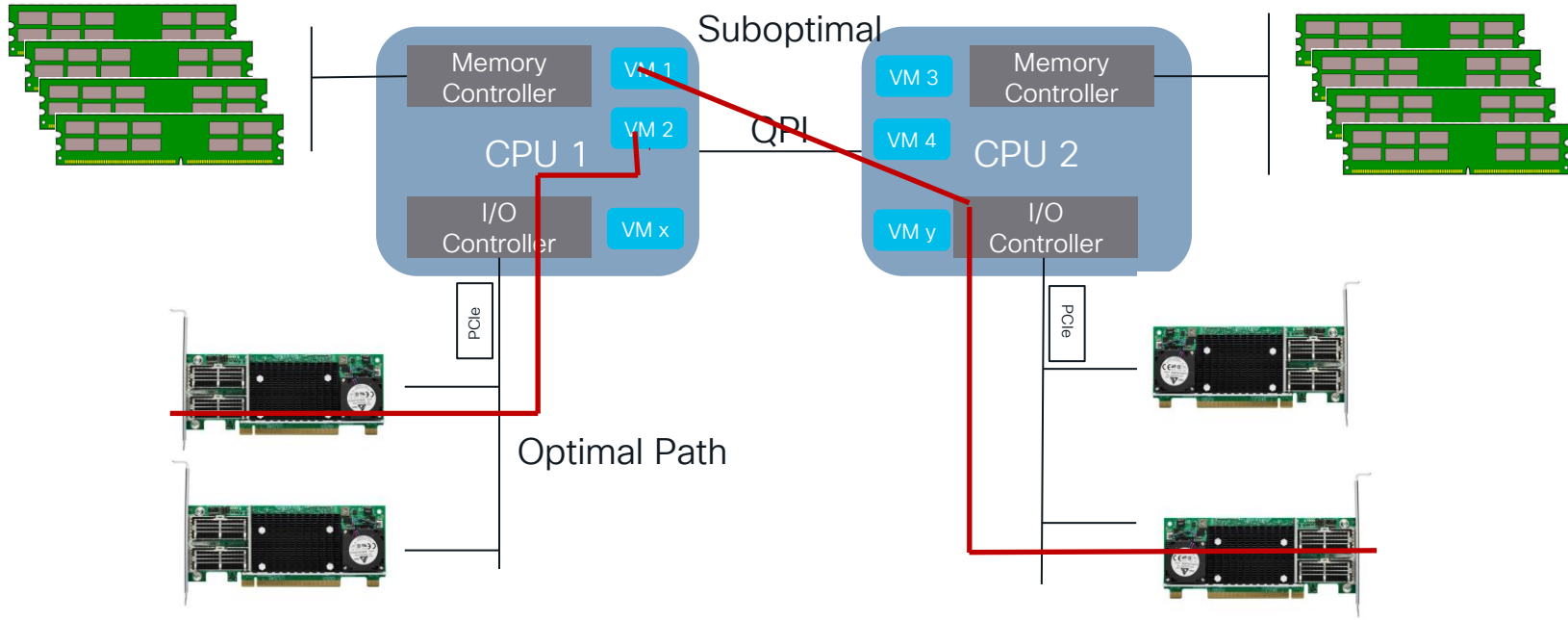


Auto Scale

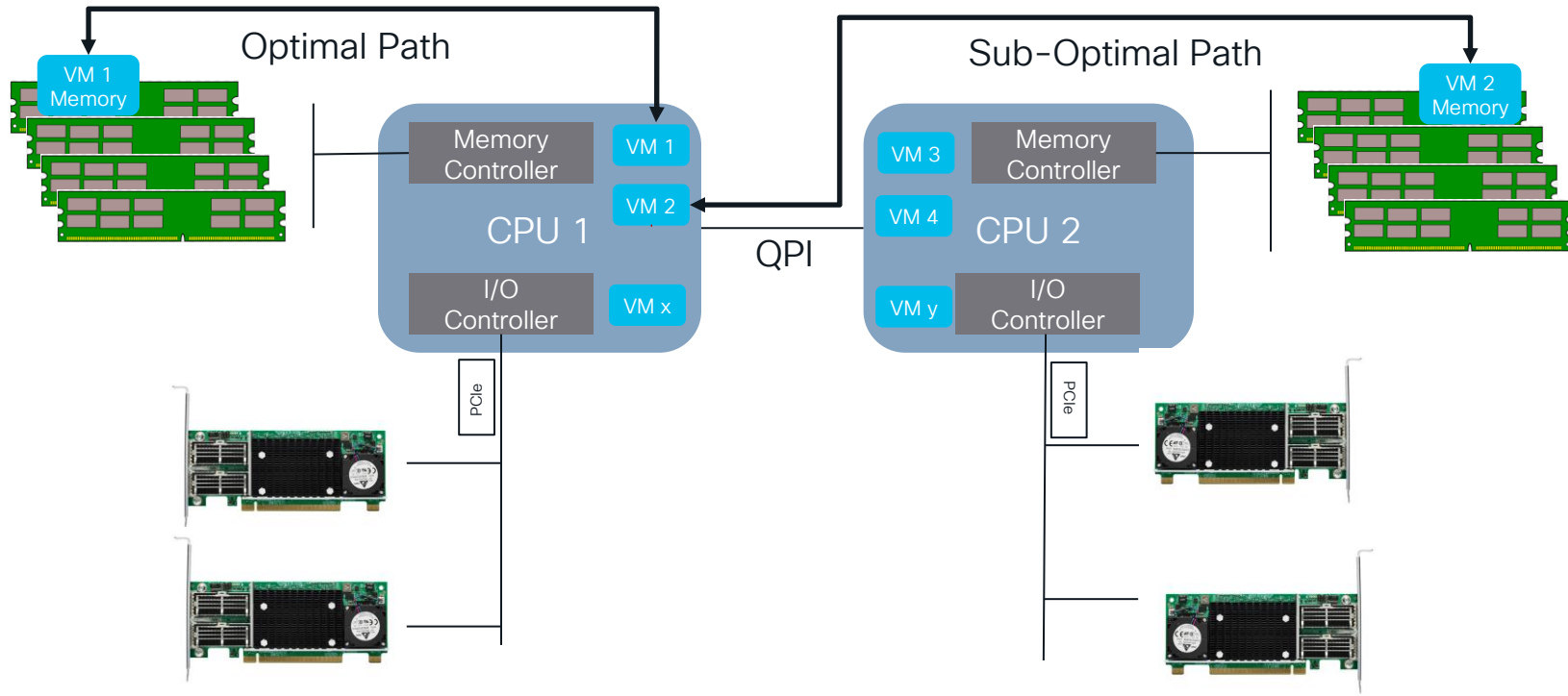
- No impact on cost, but impacts available resources.
- Not all built-in capabilities like Cloud Director are supported.
- Use VNF-Manager such as ESC: Cisco Elastic Services Controller



PCIe Cards are Local to a CPU



NUMA: Memory Locality

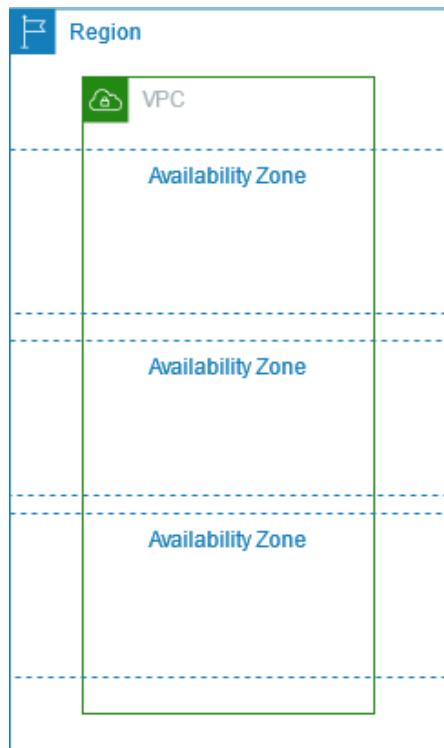


CISCO *Live!*



Designing in Public Cloud

Virtual Private Cloud (VPC)

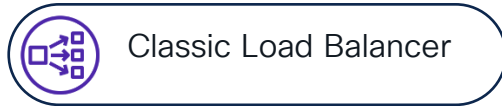


- A VPC spans all of the **Availability Zones** in a Region.
- After you create a VPC, you can add one or more subnets in each Availability Zone.
- AZ:
 - Redundant power
 - Redundant cooling
 - Redundant connectivity
- Traffic between AZ's is encrypted

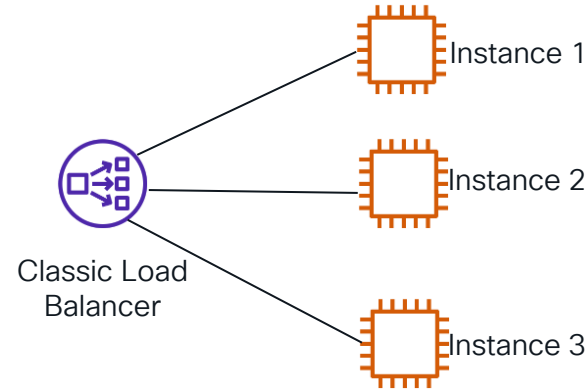
High Availability Considerations

- A lot of redundancy is built in and sometimes not immediately obvious.
- Links and interfaces are logical.
- Designing against single point of failure is different as a consequence.
- Most HA designs will have some form of load balancer involved. Understanding the sometimes subtle differences is key.

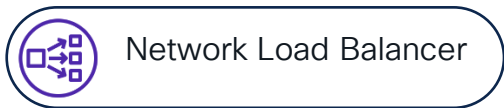
Classic Load Balancer (CLB)



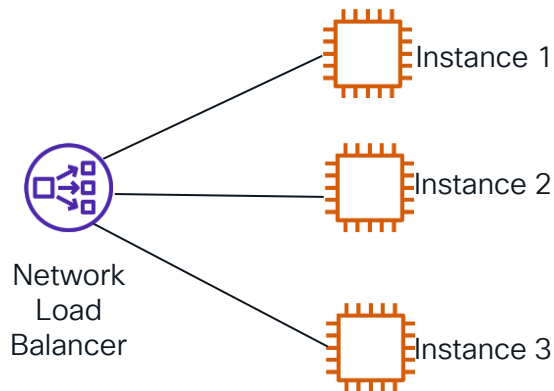
- Forwards traffic only to the primary interface of a VM in the backend pool
- Not recommended
- Works with Cisco Secure Firewall ASA only, would send to mgmt interface on FTDv



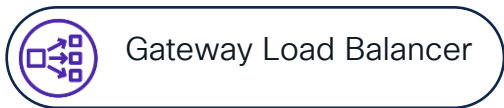
Network Load balancer (NLB)



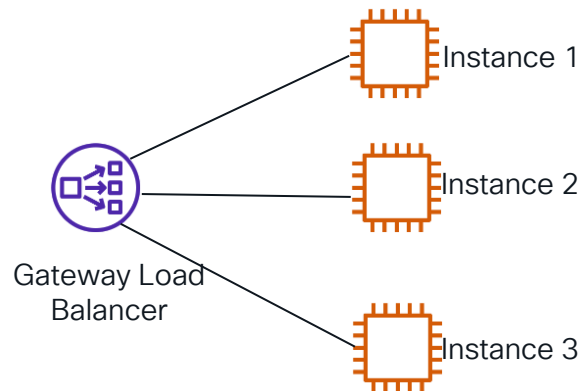
- Layer 4 TCP/UDP connection-based load balancing
- Source IP Preservation
- Health Check
- Sticky Sessions
- Zonal Isolation
- Long Live TCP connections
- Low Latency
- IP address as Targets
- TLS offloading
- Works with Cisco Secure Firewall Threat Defense and Cisco Secure Firewall ASA



Gateway Load balancer (GWLB)



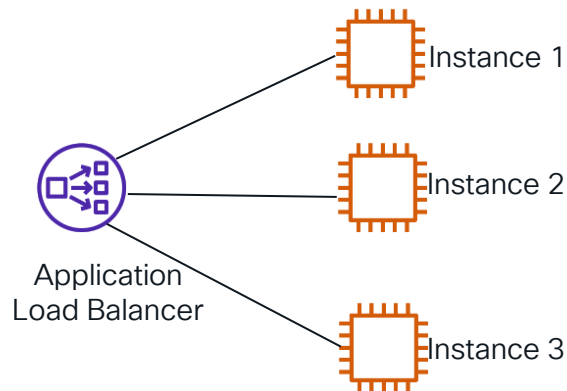
- Layer 3 load balancing
- Source IP Preservation
- Health Check
- Sticky Sessions
- Zonal Isolation
- Long Live TCP connections
- Source & Destination are unaware the traffic is inspected
- Geneve Encapsulation packet is preserved
- Works with Cisco Secure Firewall Threat Defense and Cisco Secure Firewall ASA*



Application Load balancer (ALB)



- Layer 7 (HTTP/HTTPS) connection-based load balancing
- Support for HTTP 1.1 & HTTP 2
- Content-based routing
- Health Check
- Sticky Sessions
- Works with Cisco Secure Firewall Threat Defense and Cisco Secure Firewall ASA



High Availability: Use Clustering

- No regular L2 so regular failover is not an option.
- Clustering instead for High Availability.
 - 7.2 minimum version for AWS and GCP, 7.3 for Azure
 - Clusters up to 16 nodes for Azure, GCP and AWS
 - Clusters up to 4 nodes for VMware and KVM
 - No auto scale support.

Clustering: Physical vs Cloud

Physical FTD Cluster

Data interfaces have two modes:

Individual interface mode – different nodes have different IP on data interfaces.

Spanned interface mode – all nodes share a VIP for each data interface.

Spanned interface mode is far more common. It uses EtherChannel for load balancing traffic coming to and from the switching infrastructure.

The CCL uses a proprietary protocol encapsulated in IP.

Cisco recommends increasing the MTU of the CCL by 100 bytes to accommodate the cluster metadata header.

The CCL uses multicast to discover and monitor cluster nodes. This allows dynamic node discovery.

Virtual FTDv Cluster

The cluster only uses **individual interface mode**. You will need a layer 3 (or higher) load balancer load balances the traffic.

The CCL link uses VXLAN over UDP as most clouds will not touch L4 headers.

Cisco recommends increasing the MTU of the CCL by 150 bytes to accommodate the cluster metadata header and the VXLAN header.

The CCL uses unicast to discover and monitor cluster nodes. This requires a static list of candidate peer IP addresses, called a **peer group**.

Clustering Configuration

Public Cloud

Do **not** use the FMC for initial cluster configuration.

Use day-0 configuration to bootstrap the cluster.

You must register a single cluster node to the FMC.

The FMC discovers the cluster and automatically registers the remaining nodes.

Use the FMC for remaining configuration.

Private Cloud

Use the FMC for initial cluster configuration.

You do not need to use any day-0 configuration to bootstrap the cluster.

You must register each cluster node separately to the FMC.

Once you register all the nodes, you create the cluster using the FMC.

Use the FMC for remaining configuration.

That's a lot of Work ...

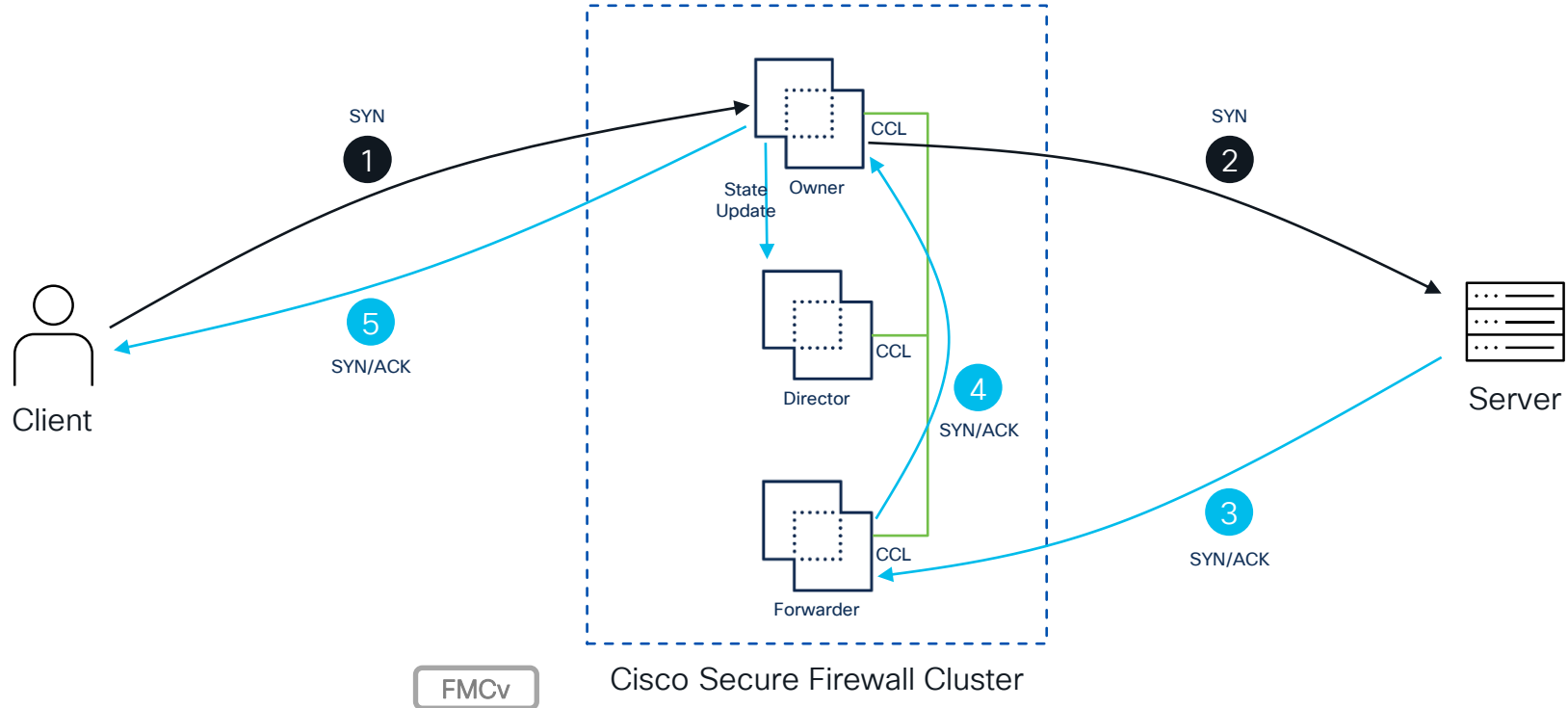


Automation is here to help.

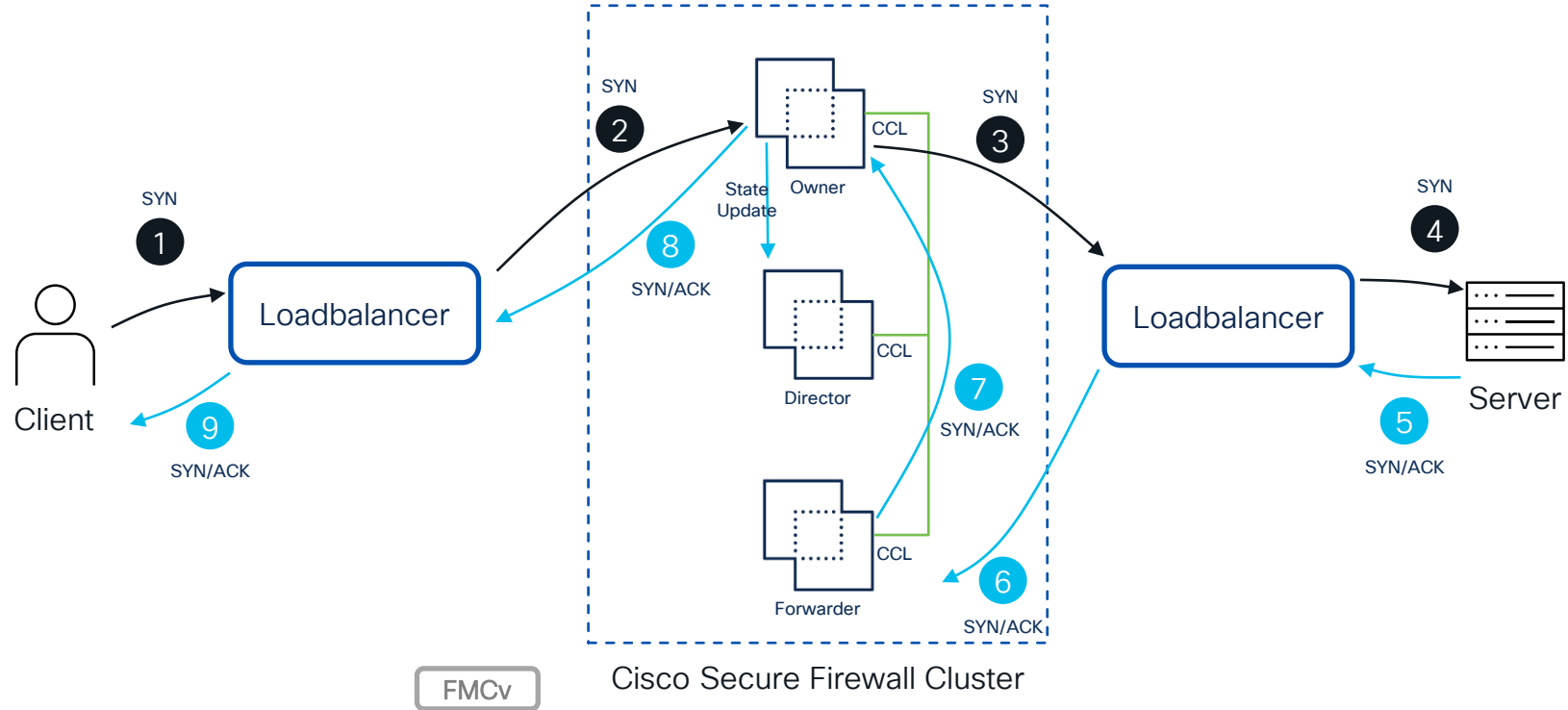
└─ And it's relatively easy!



Physical Firewall Clustering Overview



Virtual Firewall Clustering Overview



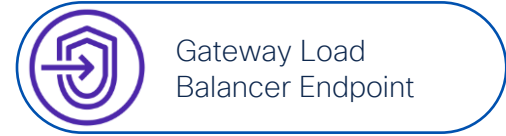
Cisco Secure Firewall Threat Defense

AWS Gateway Load Balancer (GWLB) Integration Overview

- ▶ The new approach to load balancing
 - AWS introduced it in November 2020
- ▶ Provides transparent insertion of services
 - The right way to do load balancing between firewalls
 - The right way to service chaining in the public cloud
- ▶ GWLB encapsulates traffic before sending it to the targets on the same subnet
 - A firewall does not need to apply NAT or routing to traffic
- ▶ GWLB deployment varies significantly between public cloud providers
- ▶ GWLB uses GENEVE protocol, and support for GENEVE on Cisco Secure Firewall Threat Defense is available from release 7.1
- ▶ **Support for Autoscale Deployment is available from release 7.2**



Gateway Load
Balancer



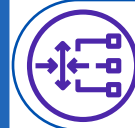
Gateway Load
Balancer Endpoint

Cisco Secure Firewall Threat Defense

AWS Gateway Load Balancer (GWLB) Integration Overview

- ▶ The new approach to load balancing
 - AWS introduced it in November 2020
- ▶ Provides transparent insertion of services
 - The right way to do load balancing between firewalls
 - The right way to service chaining in the public cloud
- ▶ GWLB encapsulates traffic before sending it to the targets on the same subnet
 - A firewall does not need to apply NAT or routing to traffic
- ▶ GWLB deployment varies significantly between public cloud providers
- ▶ GWLB uses GENEVE protocol, and support for GENEVE on Cisco Secure Firewall Threat Defense is available from release 7.1
- ▶ **Support for Autoscale Deployment is available from release 7.2**

Read:
The Native
Cloud way



Gateway Load
Balancer



Gateway Load
Balancer Endpoint

Cisco Secure Firewall Threat Defense

AWS Gateway Load Balancer (GWLB) Integration Overview

GENEVE

- ▶ Stands for Generic Network Virtualization Encapsulation
- ▶ Designed to accommodate network virtualization changing capabilities and needs
- ▶ Provides flexible and extensible data format

Added in FTD release 7.1

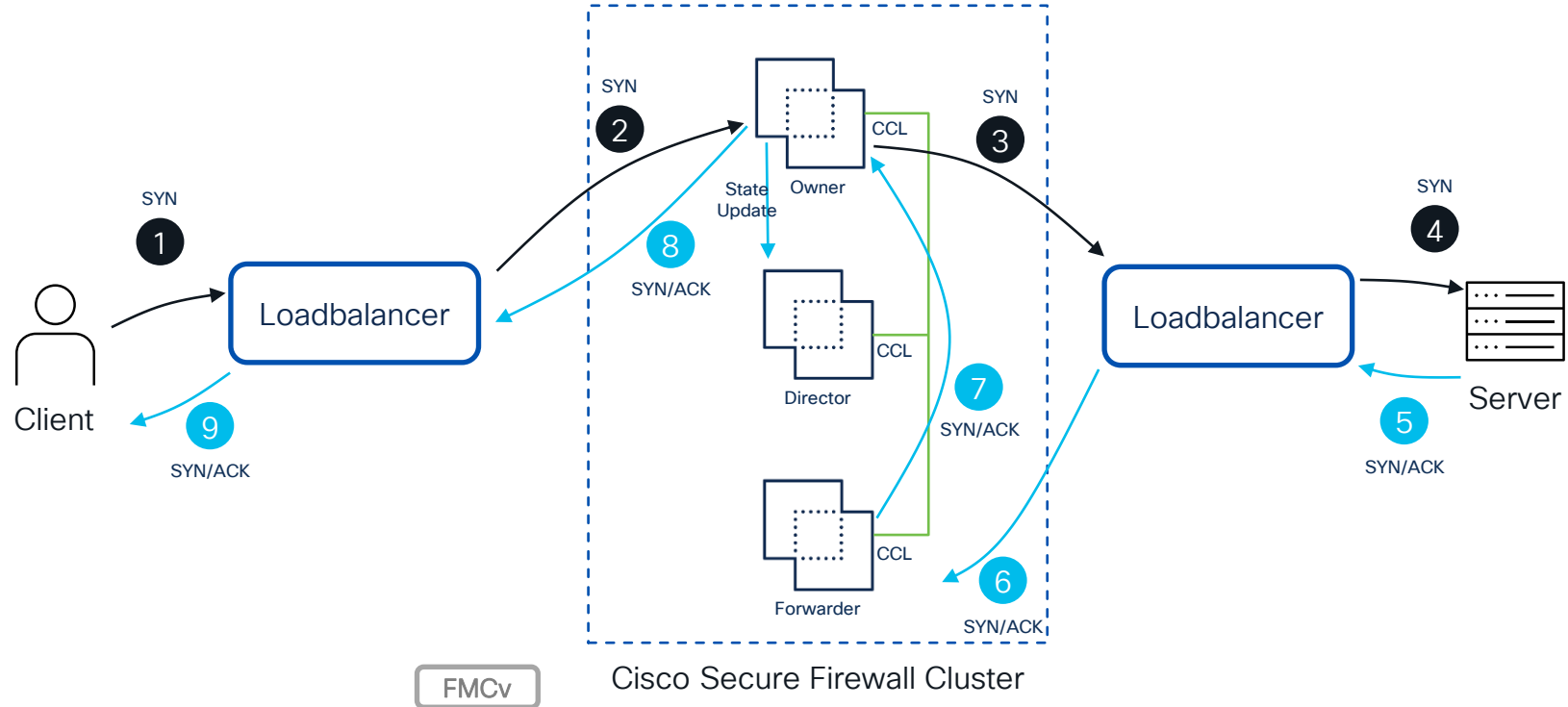
- ▶ Cisco Secure Firewall can terminate GENEVE tunnels
- ▶ Allows integration with AWS Gateway Load Balancer
- ▶ Implemented using VNI interface with NVE



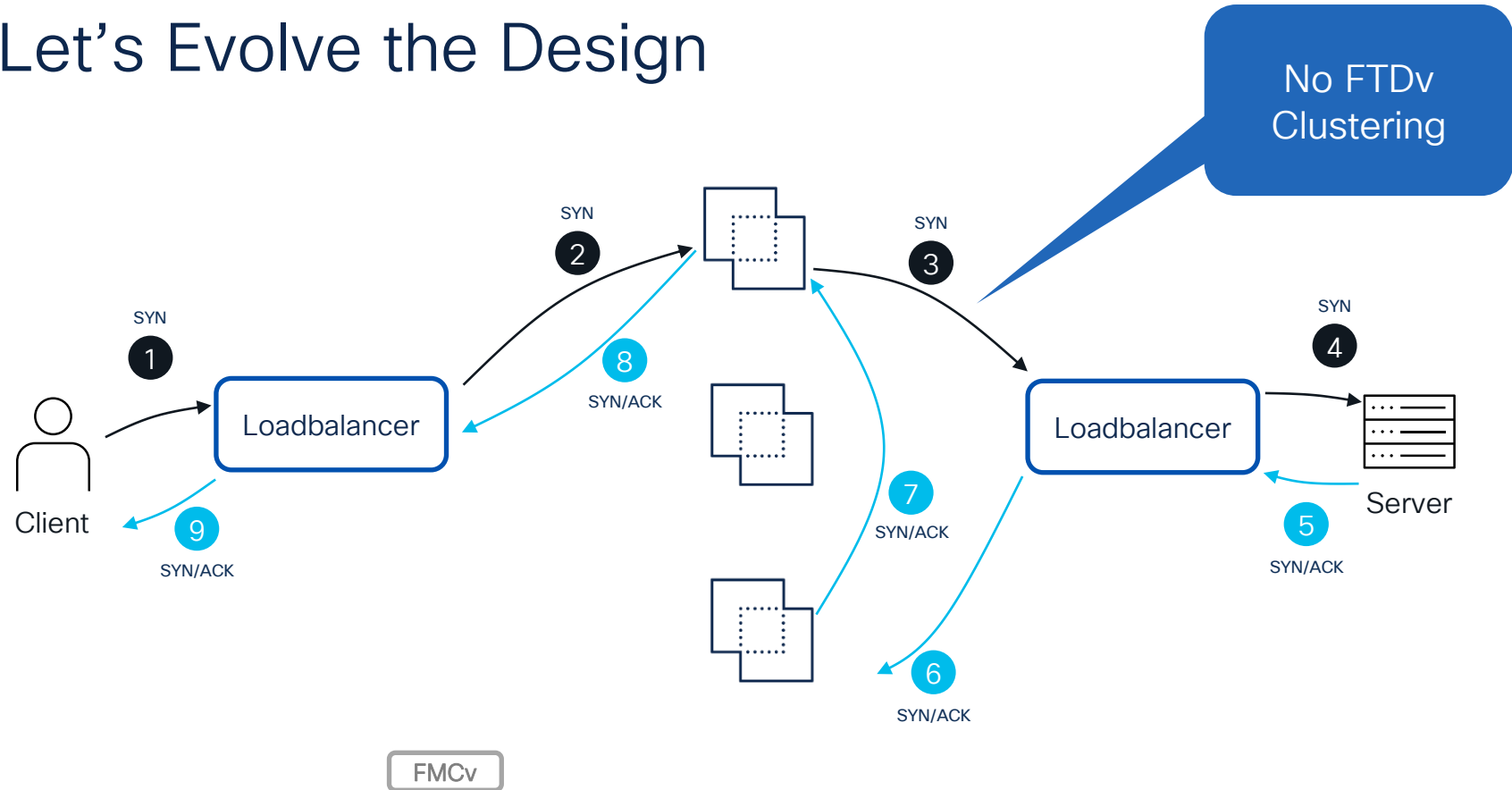
Flexible Inner Header Setting Defined by GENEVE Header



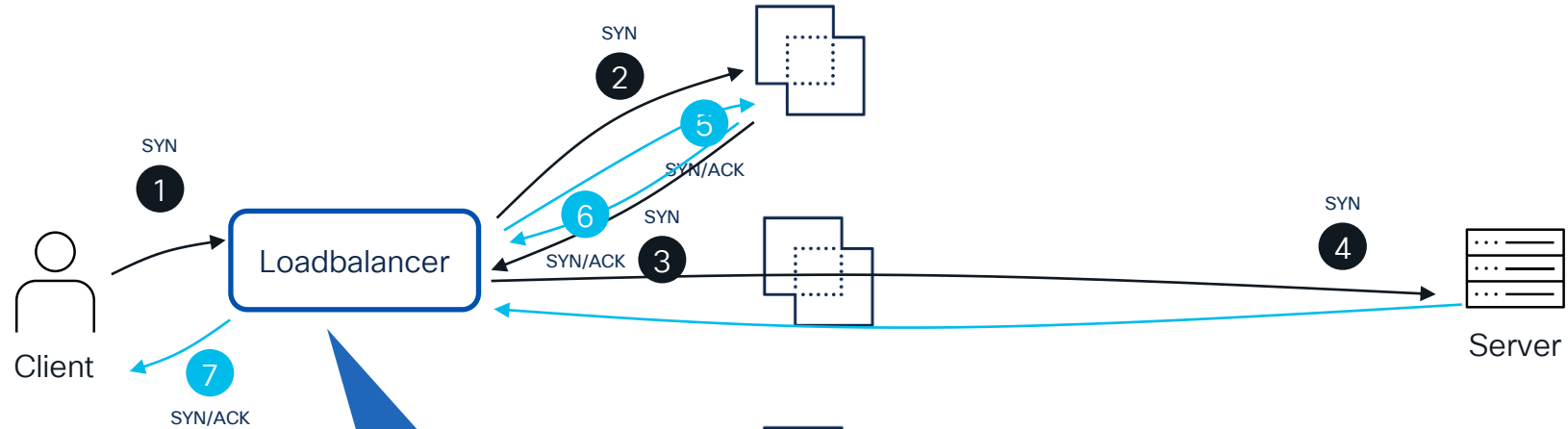
Let's Evolve the Design



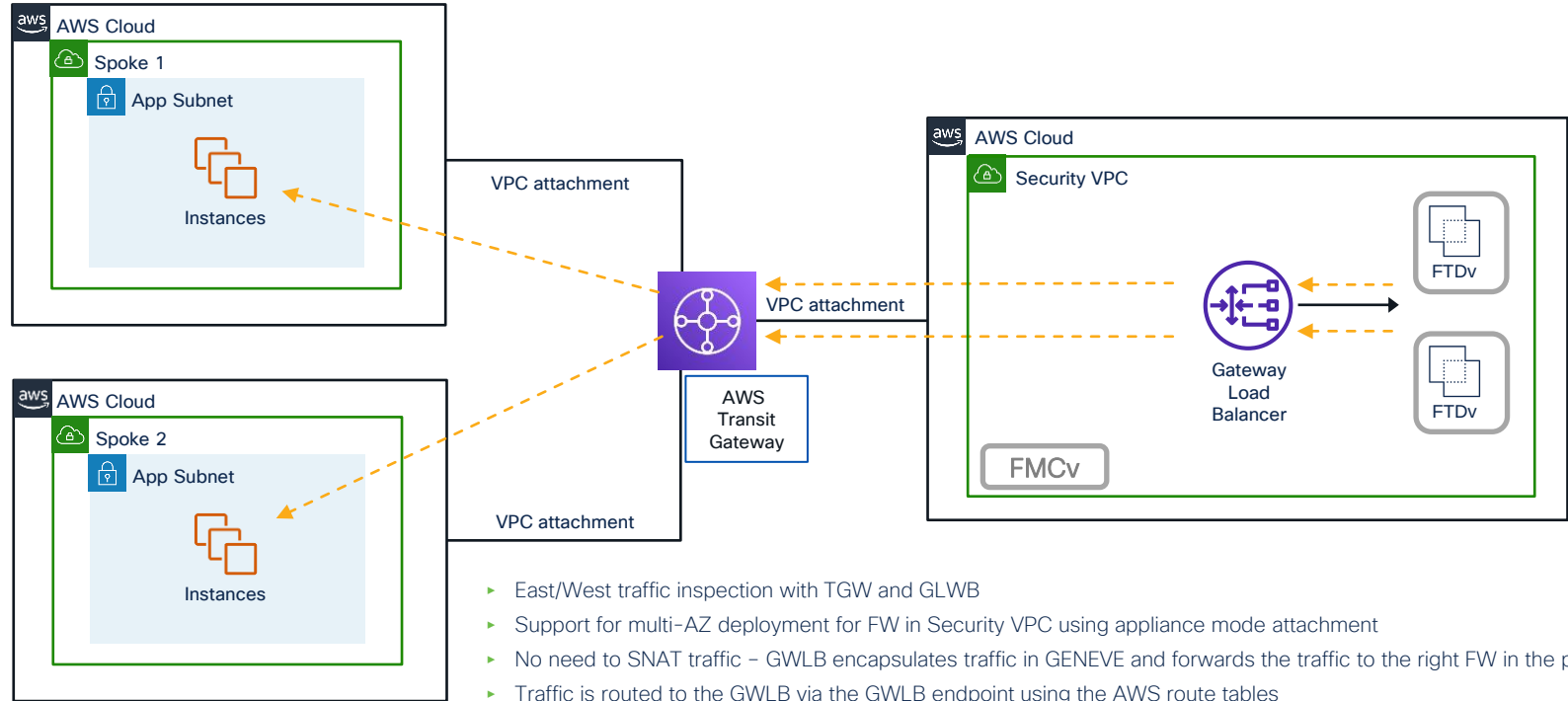
Let's Evolve the Design



Let's Evolve the Design

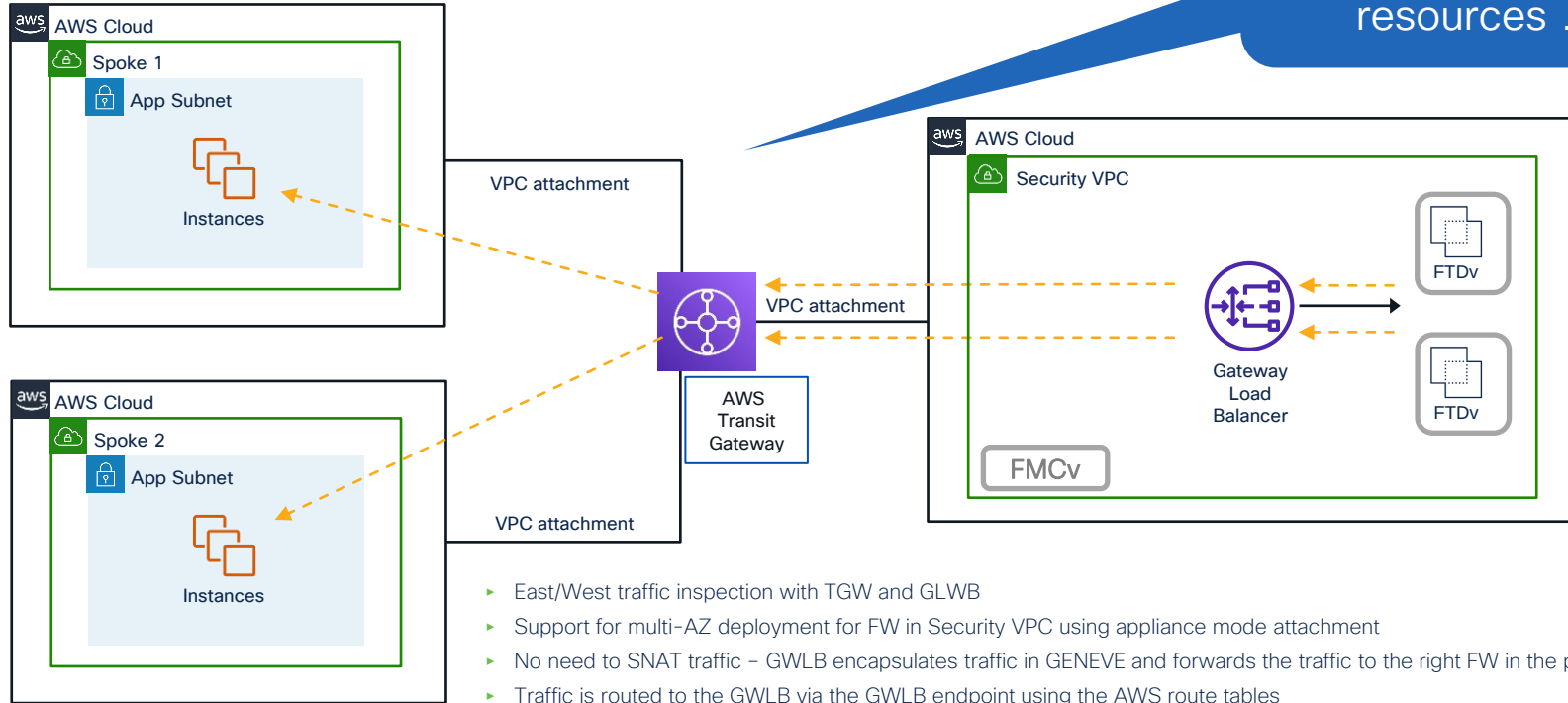


FTDv Loadbalancer Design with AWS



FTDv Loadbalancer Design with AWS

Initial deployment
requires over a 100
resources ...



That's a lot of Work ...

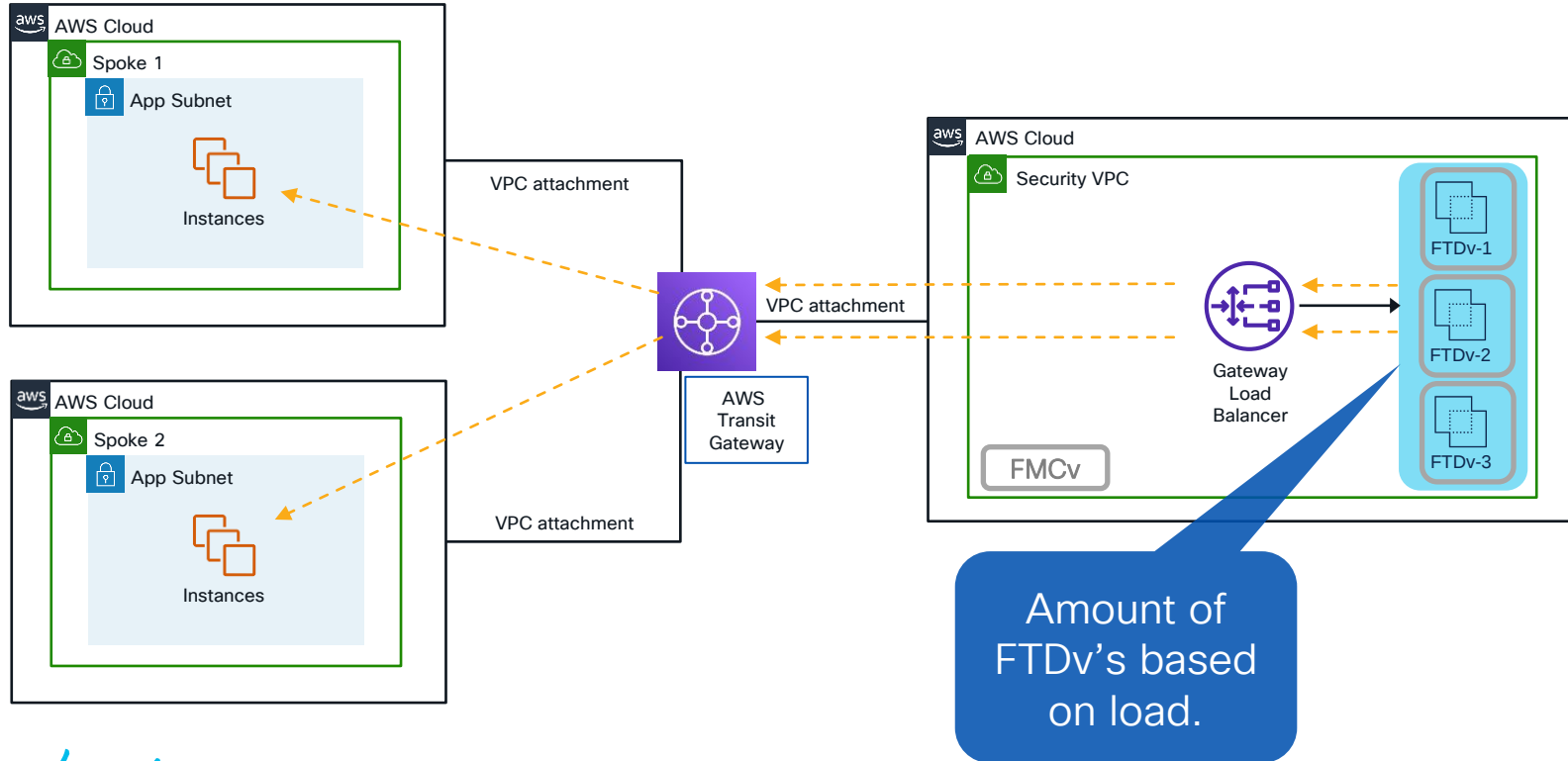


Automation is here to help.

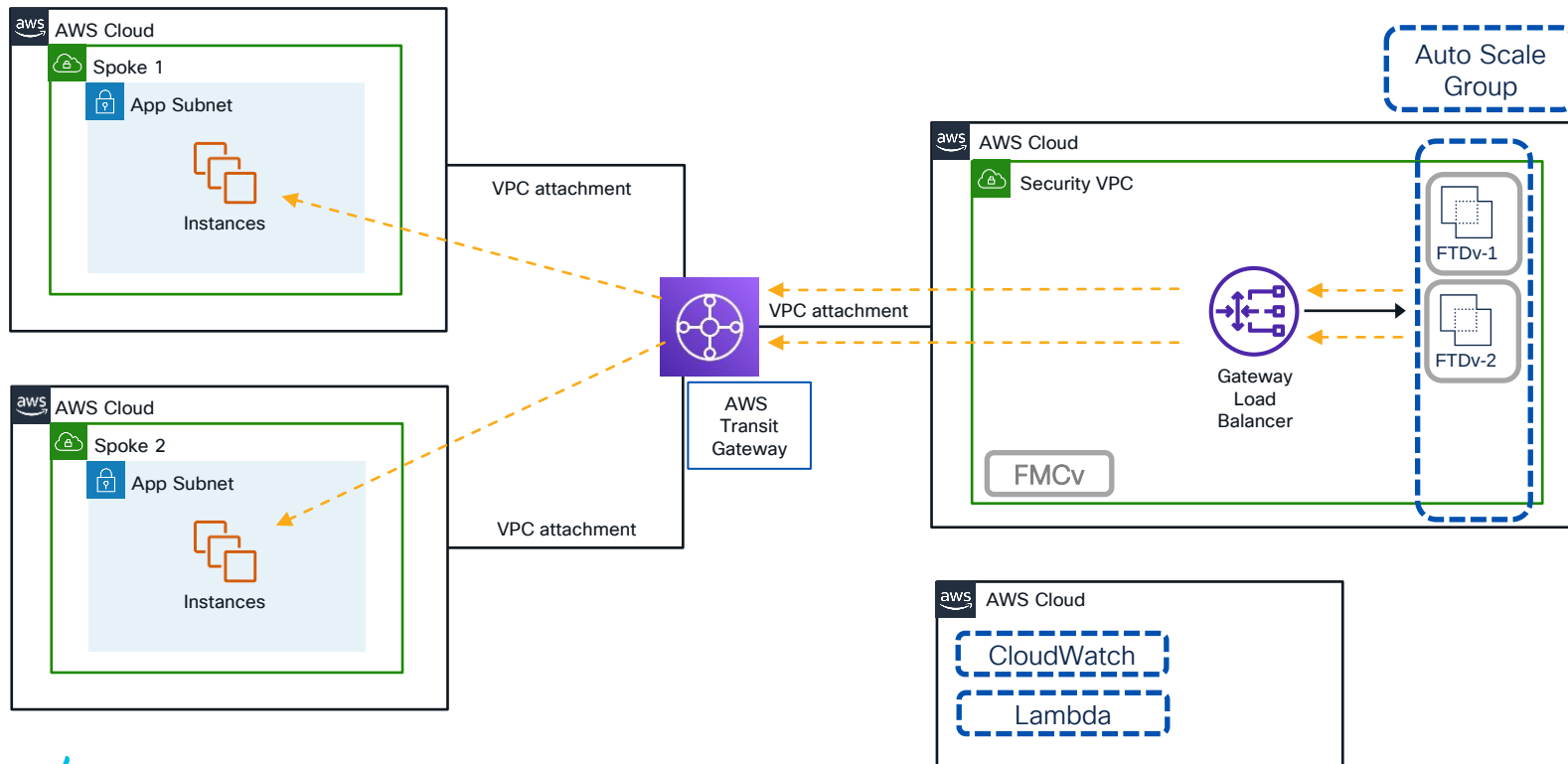
└─ And it's relatively easy!



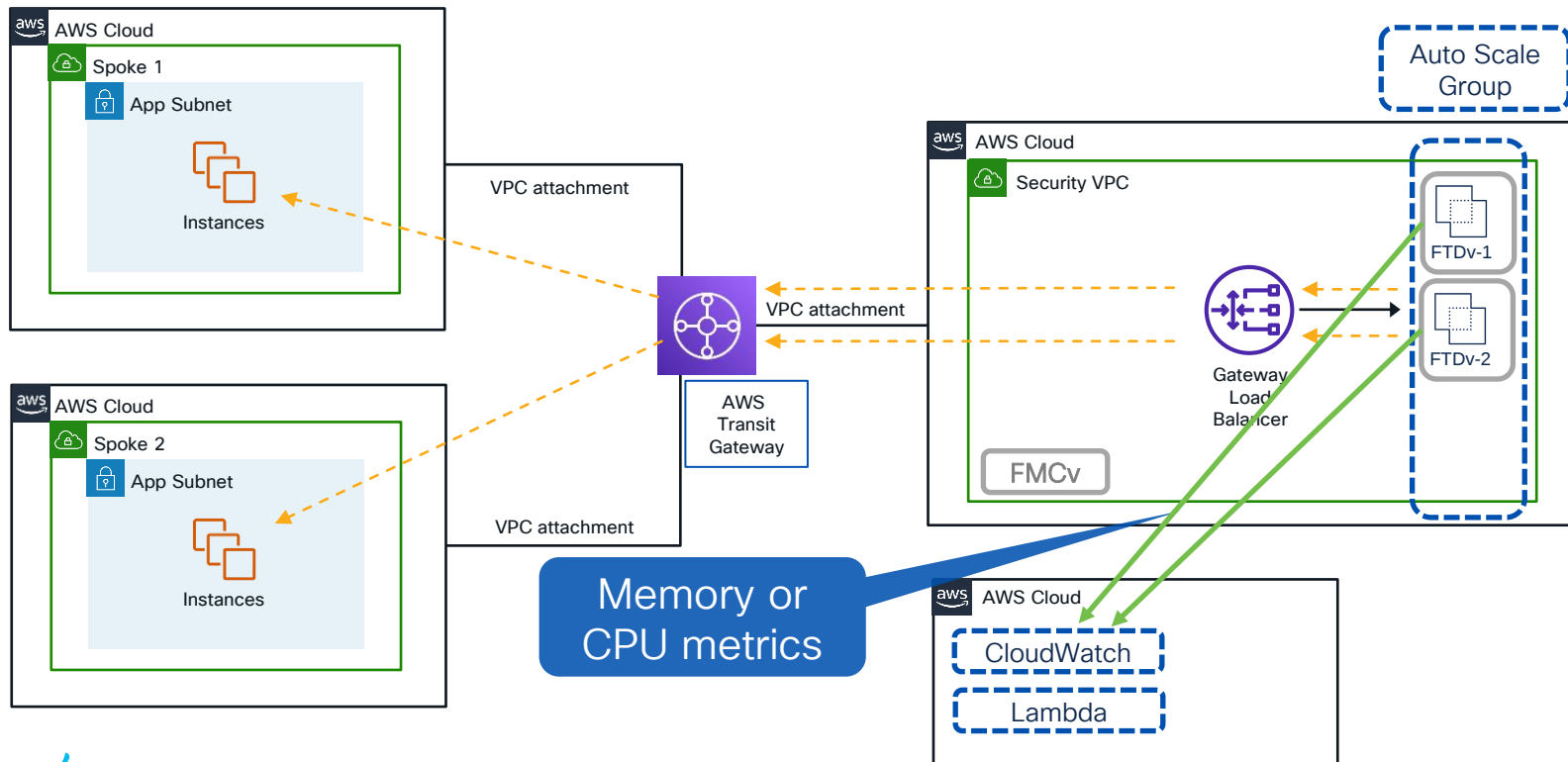
Let's add Elasticity, aka Auto Scaling



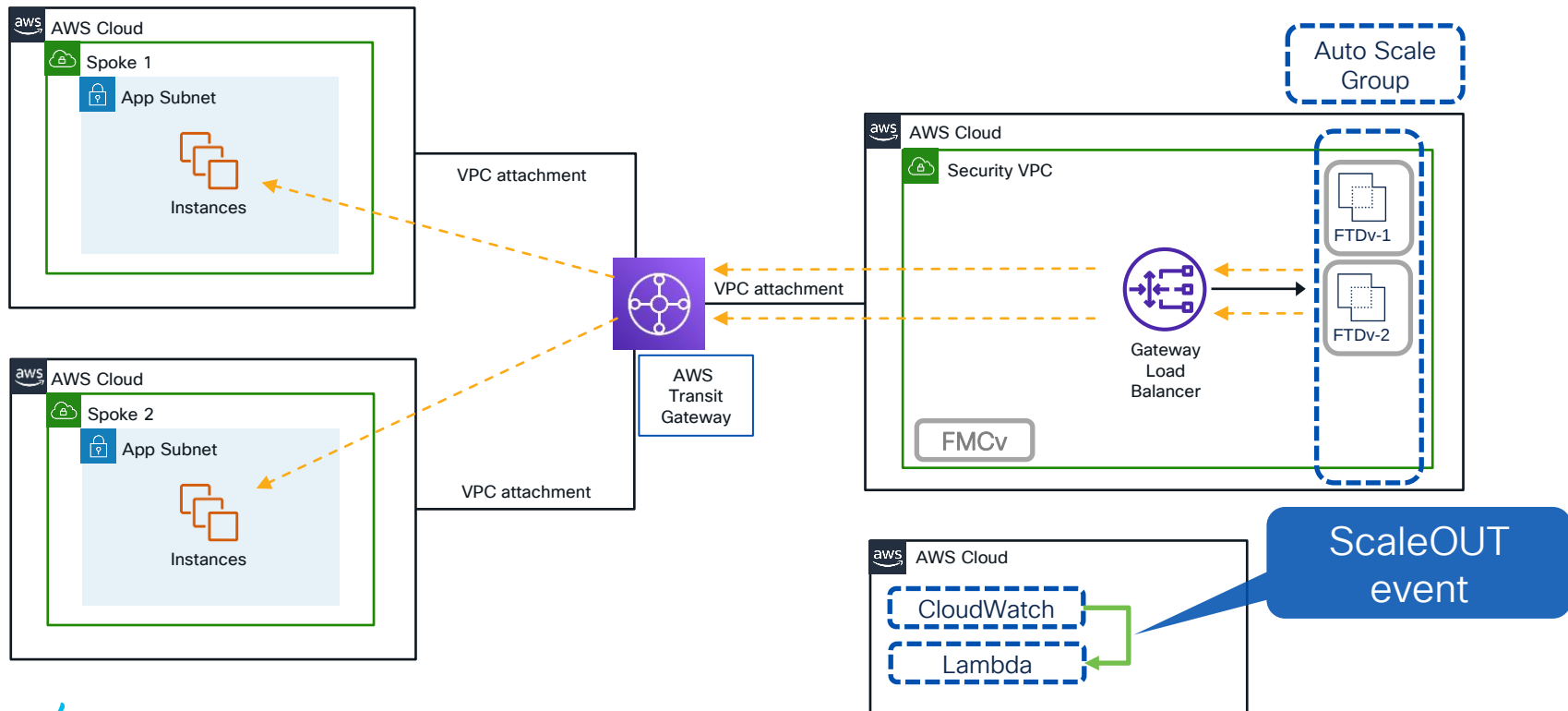
Auto Scale



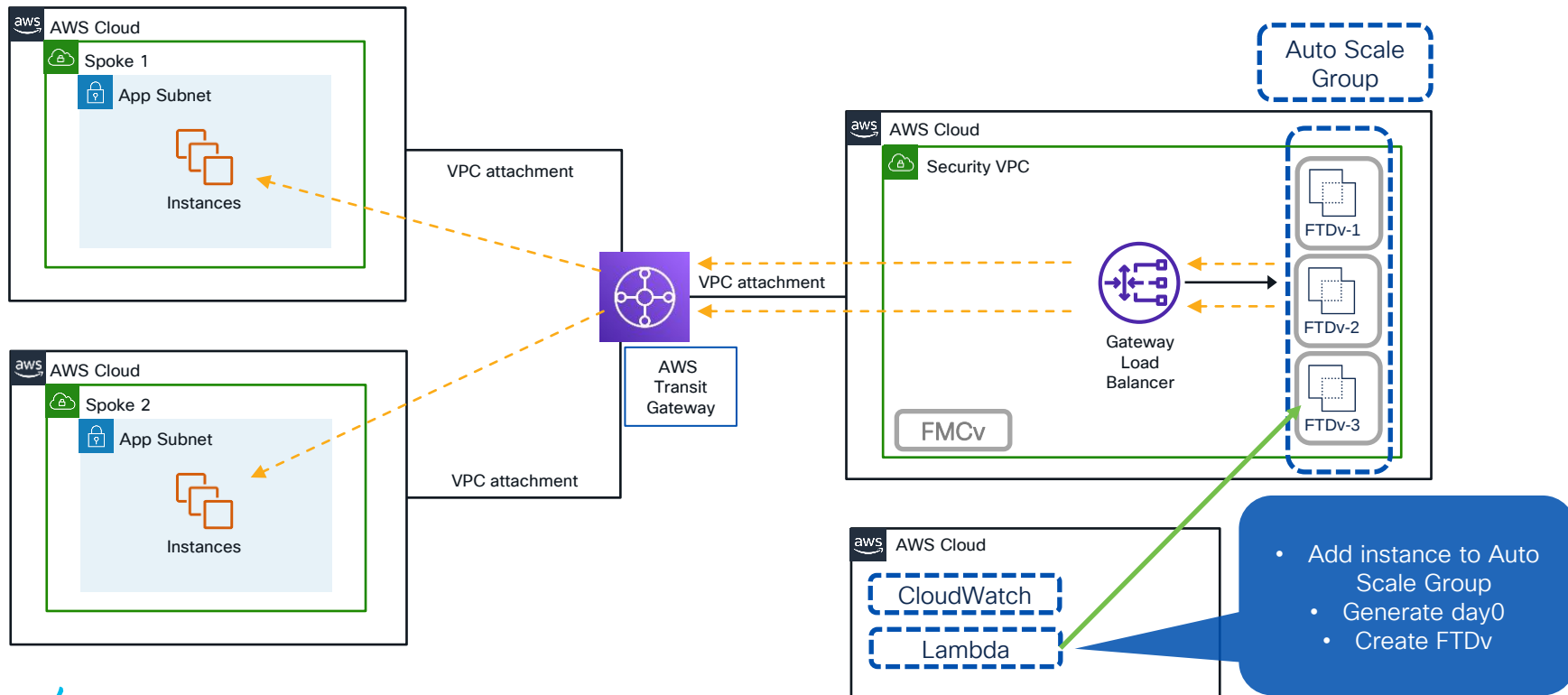
Auto Scale: What's Going On?



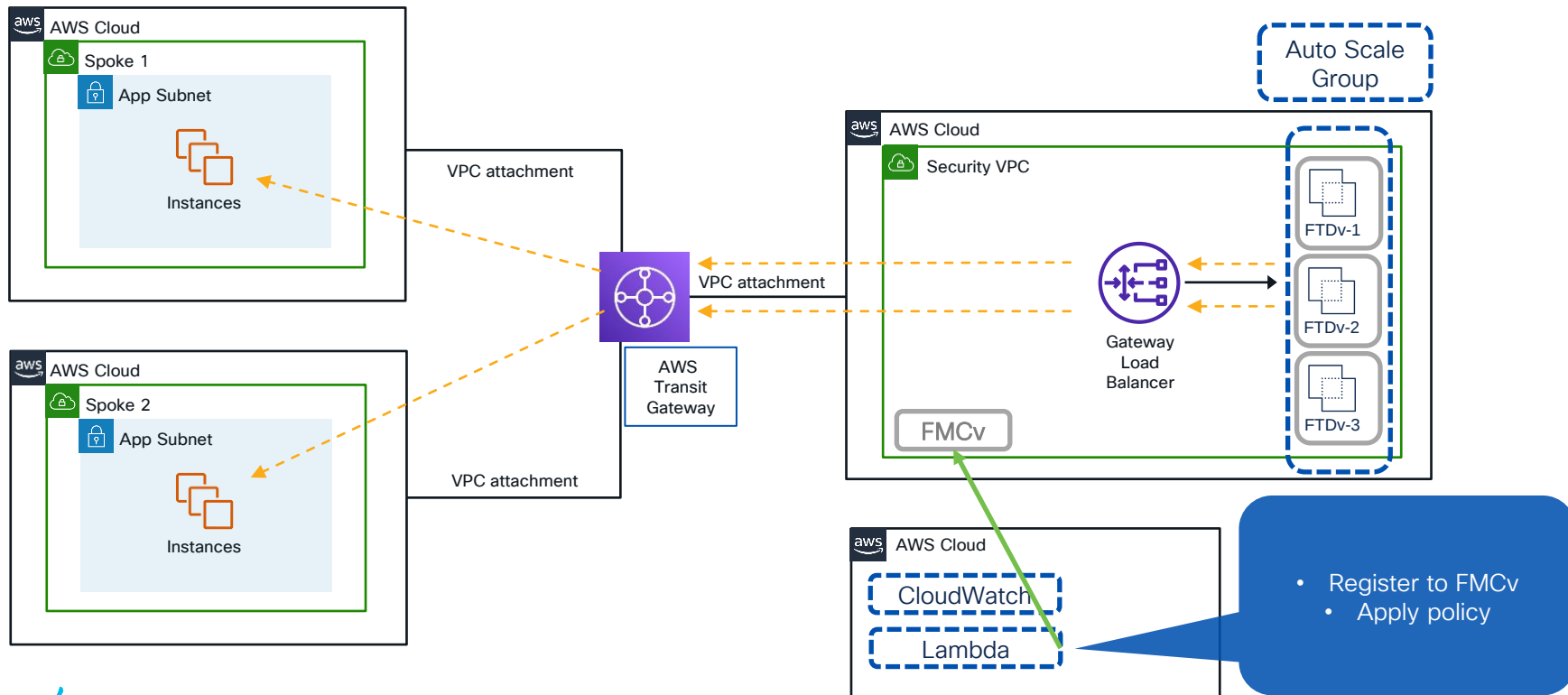
Auto Scale: What's Going On?



Auto Scale: What's Going On?



Auto Scale: What's Going On?



That's a lot of Work ...



Automation is here to help.

└─ And it's relatively easy!



Cisco Secure Dynamic Attribute Connector (CSDAC)

Aggregates dynamic attributes from public and private cloud for Secure Firewall Policy.

Deployment Scenario

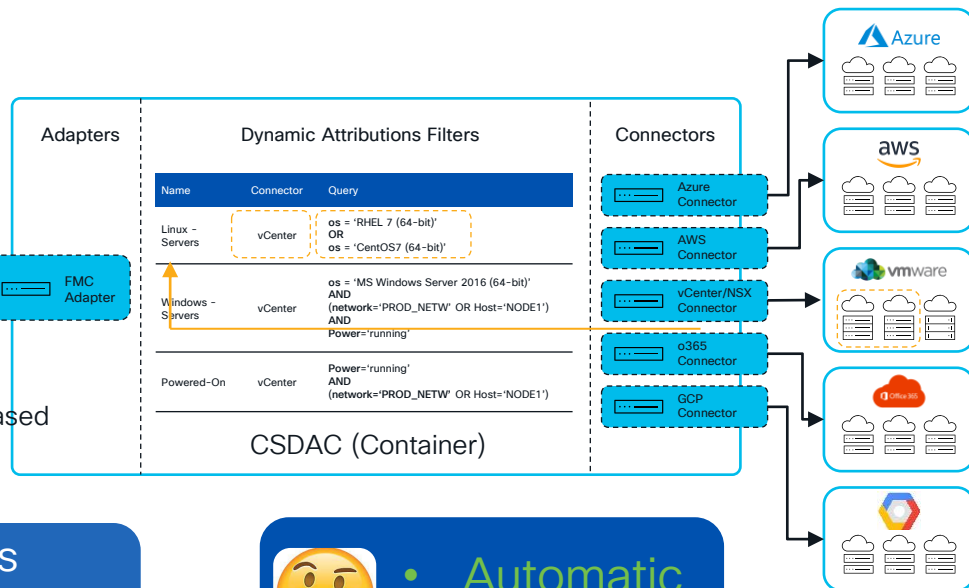
- ▶ Create dynamic policy for On-prem and Cloud elements
- ▶ Dynamic object for SaaS applications e.g., O365 etc.

Dynamic Object	Mappings
Linux - Servers	172.16.0.1
	172.16.0.3
Windows - Servers	10.0.1.11 10.0.1.14 10.0.1.20
Powered-On	10.0.1.14

Benefits

- ▶ Accelerate integration
- ▶ Adapt to changes instantaneously
- ▶ Prevent build-up of outdated firewall rules
- ▶ Control access to Office 365 and GitHub with community-based security feeds
- ▶ Accelerate your digital transformation
- ▶ Filter attributes with meaningful logical context

FMC learns automatically about new objects



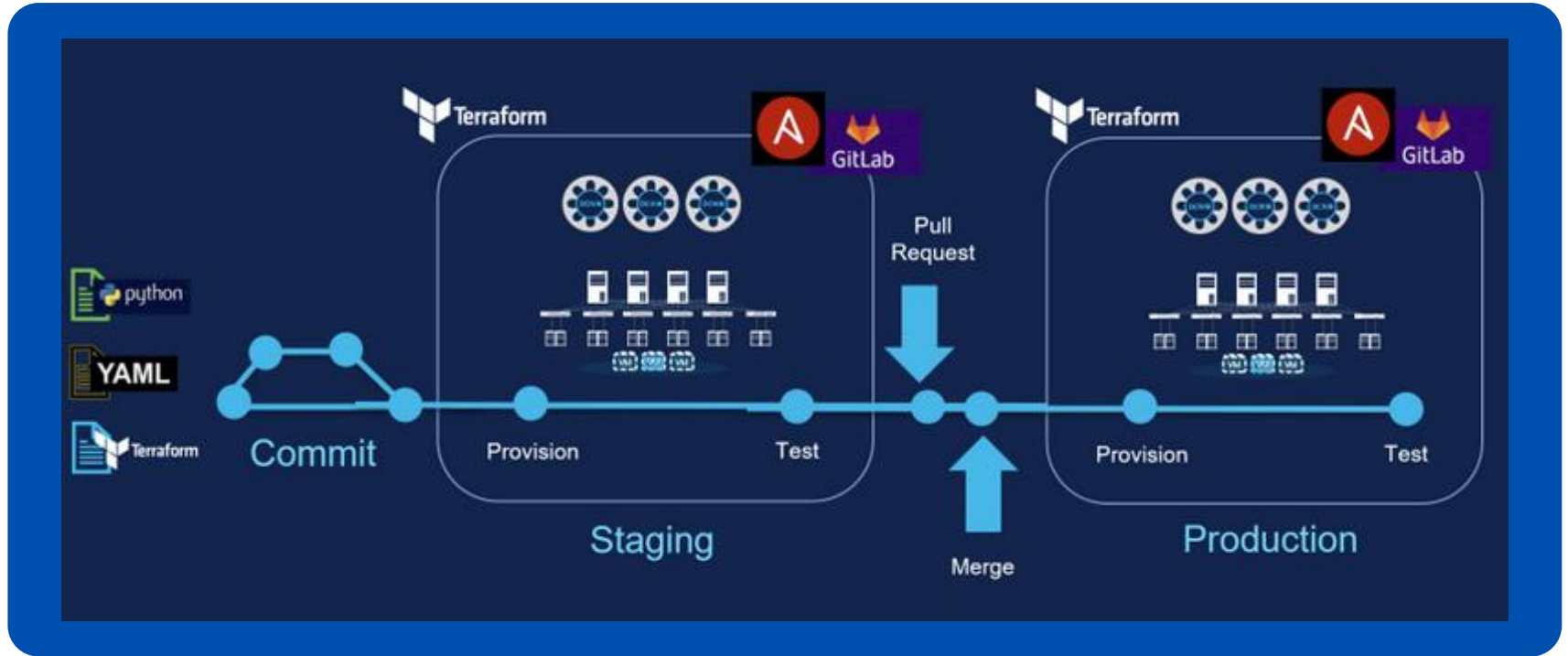
• Automatic
• Easy

Infrastructure as Code

It's easy!



Infrastructure as Code



[3 Ways for Network Practitioners to Embrace DevOps with Infrastructure-as-Code](#)

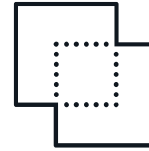
Why?



DevSecOps:
Security as Code



IaC:
Infrastructure as Code



Policy as Code

These all depend on certain capabilities to exist.
Ansible, Terraform, Git and API access are the popular tools.

Toolbox

Create infrastructure



- ▶ Create FTDv, ASAv and FMC
- ▶ On Private Cloud: Vmware, KVM
- ▶ On Public cloud: AWS, Azure, GCP,

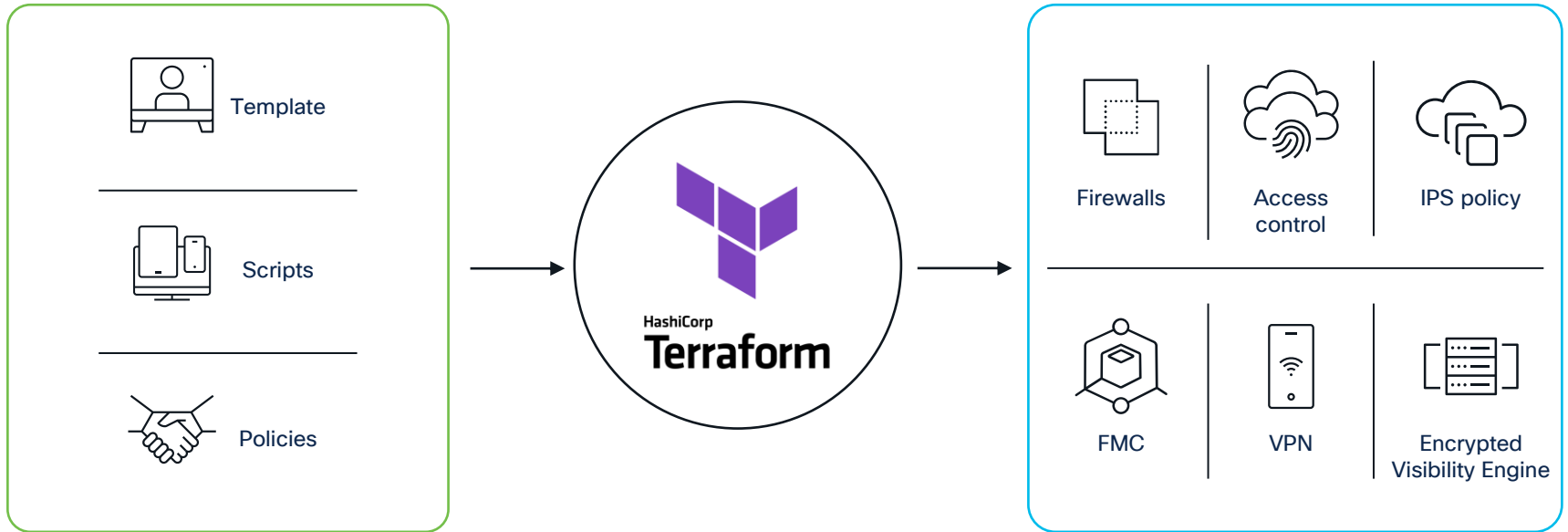
...

Manage with:



Terraform

How does Terraform work?



Automation in AWS using Terraform

Terraform templates provide the flexibility of instances, location, high availability and other factors during deployment, with ease using the same code.

<https://github.com/CiscoDevNet/secure-firewall/tree/main/FTD/AWS/Terraform>

- ▶ Deploy 'n' instances of Cisco Secure Firewall Threat Defense Virtual instances across different Availability Zones
- ▶ External load balancer to distribute traffic among different instances
- ▶ Routing table attachment to subnets
- ▶ Public IP attachment to each Cisco Secure Firewall Threat Defense Virtual instance.

```
JWITTOCK-M-M4X7:FTD_FMC_A_A_Multiple_AZ jwittock$ terraform init

Initializing the backend...

Initializing provider plugins...
- Reusing previous version of hashicorp/aws from the dependency lock file
- Reusing previous version of hashicorp/template from the dependency lock file
- Using previously-installed hashicorp/aws v4.63.0
- Using previously-installed hashicorp/template v2.2.0

Terraform has been successfully initialized!

You may now begin working with Terraform. Try running "terraform plan" to see
any changes that are required for your infrastructure. All Terraform commands
should now work.

If you ever set or change modules or backend configuration for Terraform,
rerun this command to reinitialize your working directory. If you forget, other
commands will detect it and remind you to do so if necessary.
```

Automation in AWS using Terraform

Terraform templates provide the flexibility of instances, location, high availability and other factors during deployment, with ease using the same code.

<https://github.com/CiscoDevNet/secure-firewall/tree/main/FTD/AWS/Terraform>

No secrets provided.

```
JWITTOCK-M-M4X7:FTD_FMC_A_A_Multiple_AZ jwittock$ terraform plan
var.aws_access_key
Enter a value: 
```

- ▶ Deploy 'n' instances of Cisco Secure Firewall Threat Defense Virtual instances across different Availability Zones
- ▶ External load balancer to distribute traffic among different instances
- ▶ Routing table attachment to subnets
- ▶ Public IP attachment to each Cisco Secure Firewall Threat Defense Virtual instance.

```
+ vpc_id = (known after apply)
}

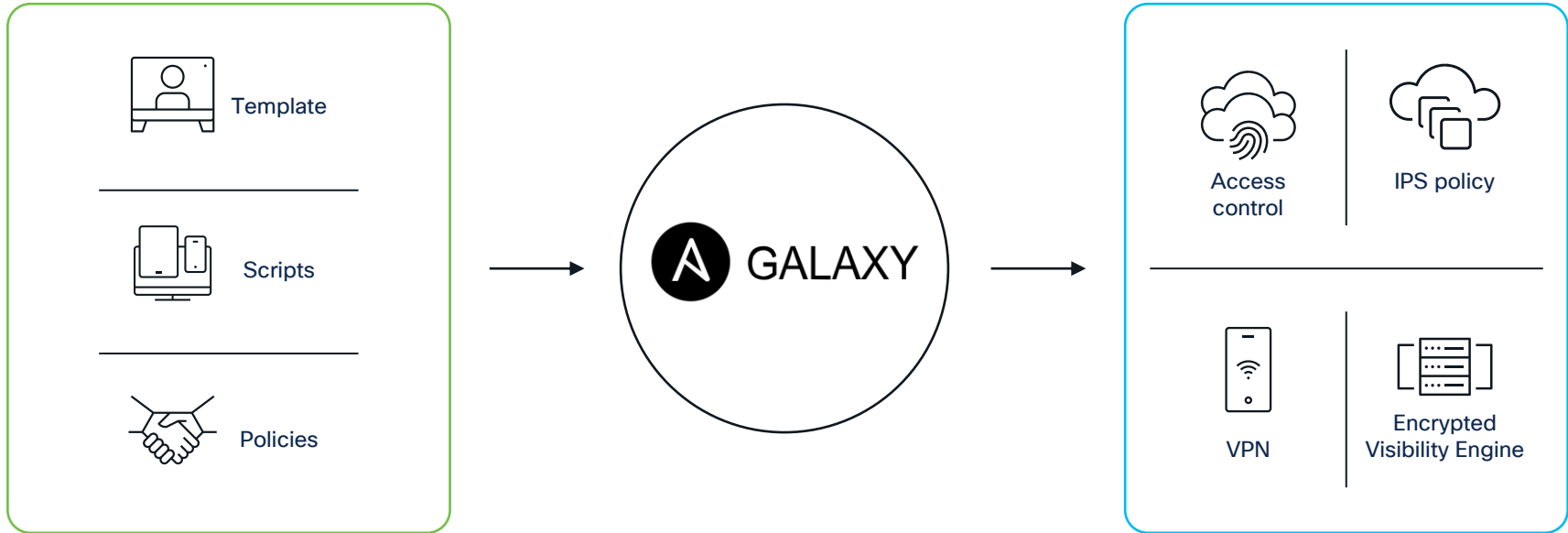
# aws_vpc.ftd_vpc will be created
+ resource "aws_vpc" "ftd_vpc" {
  + arn = (known after apply)
  + cidr_block = "172.16.0.0/16"
  + default_network_acl_id = (known after apply)
  + default_route_table_id = (known after apply)
  + default_security_group_id = (known after apply)
  + dhcp_options_id = (known after apply)
  + enable_classiclink = (known after apply)
  + enable_classiclink_dns_support = (known after apply)
  + enable_dns_hostnames = true
  + enable_dns_support = true
  + enable_network_address_usage_metrics = (known after apply)
  + id = (known after apply)
  + instance_tenancy = "default"
  + ipv6_association_id = (known after apply)
  + ipv6_cidr_block = (known after apply)
  + ipv6_cidr_block_network_border_group = (known after apply)
  + main_route_table_id = (known after apply)
  + owner_id = (known after apply)
  + tags = {
    + "Name" = "FTD-Service-VPC"
  }
  + tags_all = {
    + "Name" = "FTD-Service-VPC"
  }
}

Plan: 74 to add, 0 to change, 0 to destroy.

Changes to Outputs:
+ FMCip = (known after apply)
+ ftd01ip = (known after apply)
+ ftd02ip = (known after apply)
```

Ansible

How does Ansible work?



Firewall Management Center (FMC) Ansible

- ▶ Automates configuration management and execution of operational tasks on FMC in AWS
- ▶ This module allows the execution of all operations available in REST API in a form of Ansible tasks.
- ▶ A detailed list of supported API calls can be found on the api-explorer page of the FMC

```
JWTITTOCK-M-M4X7:FW-tools jwittock$ ansible-playbook -i inventory linux-users.yaml --ask-pass --ask-become-pass -c paramiko
SSH password:
BECOME password[defaults to SSH password]:
[WARNING]: Invalid characters were found in group names but not replaced, use -vvvv to see details

PLAY [jumphost] *****

TASK [Gathering Facts] *****
[WARNING]: Platform linux on host 10.48.138.8 is using the discovered Python interpreter at /usr/bin/python3.10, but future
interpreter could change the meaning of that path. See https://docs.ansible.com/ansible-core/2.14/reference_appendices/inte
information.
ok: [10.48.138.8]

TASK [Make sure we have a 'wheel' group] *****
ok: [10.48.138.8]

TASK [Add user accounts] *****
```

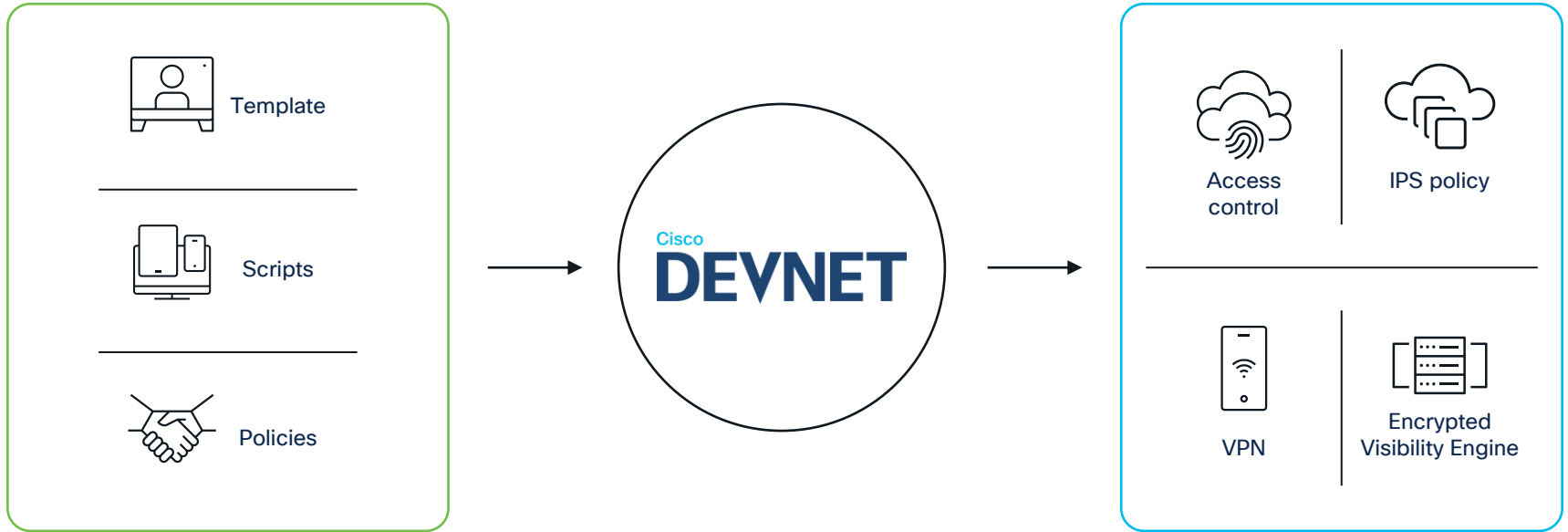
```
- name: Create Network Object
  cisco.fmcansible.fmc_configuration:
    operation: createMultipleNetworkObject
    path_params:
      domainUUID: '{{ domain[0].uuid }}'
    data:
      name: test-network
      value: 3.3.3.0/24
      type: networkobject
      register_as: test_network

- name: Create Network Object Group
  cisco.fmcansible.fmc_configuration:
    operation: createMultipleNetworkGroup
    path_params:
      domainUUID: '{{ domain[0].uuid }}'
    data:
      objects:
        - name: '{{ test_network.name }}'
          id: '{{ test_network.id }}'
```

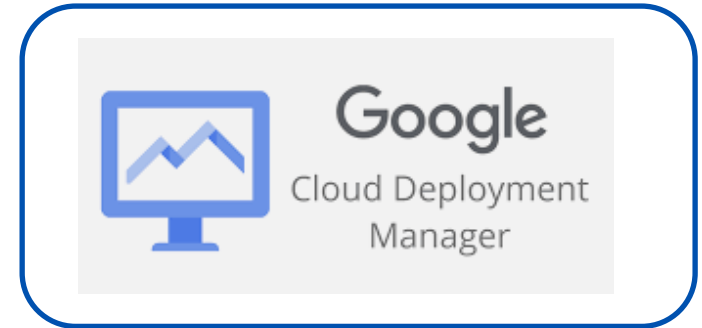
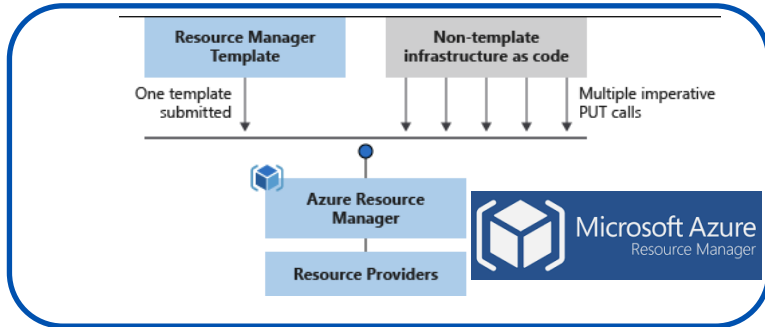
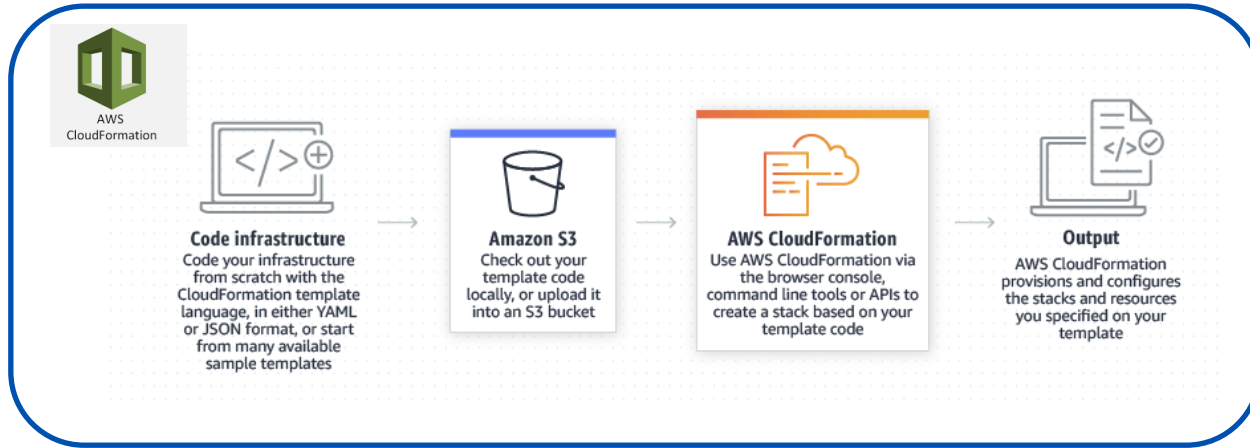
Create a Network Object Group

FMC API

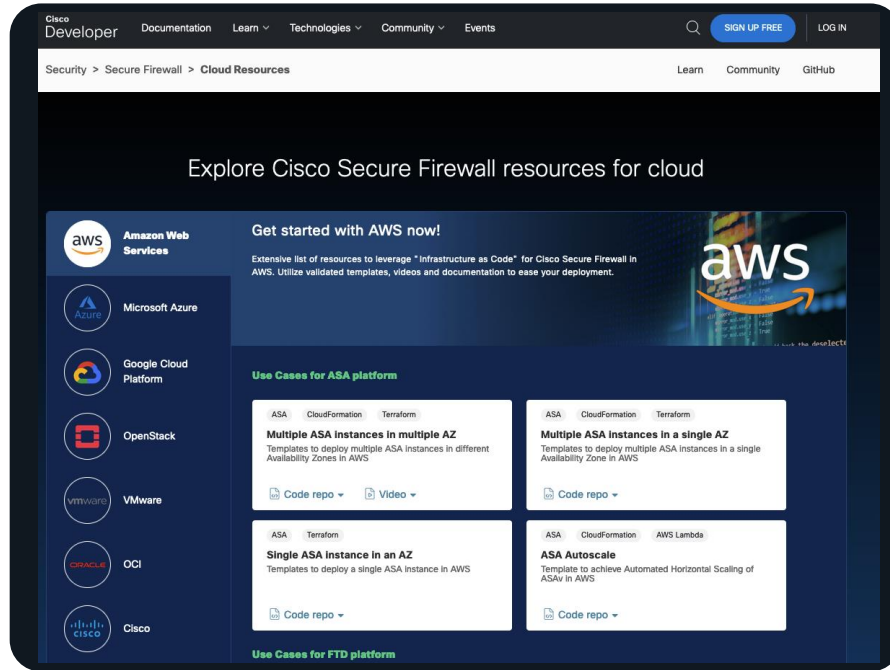
Using FMC API



Native Cloud options



Examples on Devnet



<https://github.com/CiscoDevNet/secure-firewall>

Public Resources



- ▶ [Manage FMC module](#)
[Source code: DevNet public repo](#)
- ▶ [ASA Collection](#)
[Source code: public Github](#)
- ▶ [CSDAC Role](#)
[Source code: DevNet public repo](#)



- ▶ [Manage FMC Provider](#)
[Source code](#)
- ▶ [Manage ASA Provider](#)
[Source code](#)
- ▶ [Enable CSDAC in FMC module](#)
[Source code](#)
- ▶ [Module to deploy FTD and FMC on AWS](#)
[Source code](#)

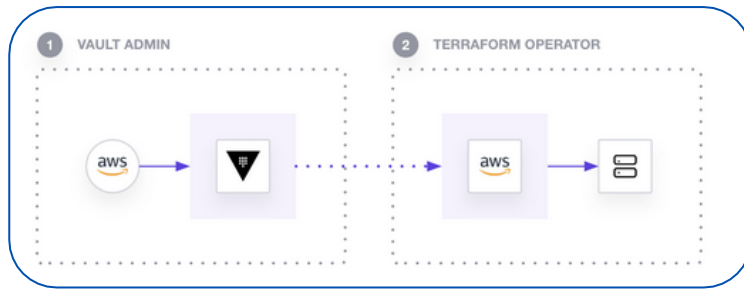


- ▶ [Manage FTD module](#)

Secrets Management

- Don't hardcode in your scripts!
- Better: Use environment variables
- Even better, aka Best: Dedicated secret management tool.

For example: Vault has a Terraform provider



1. Configure AWS secrets in Vault
2. Connect to Vault when access to secrets is required.

Conclusion

Fill out your session surveys!



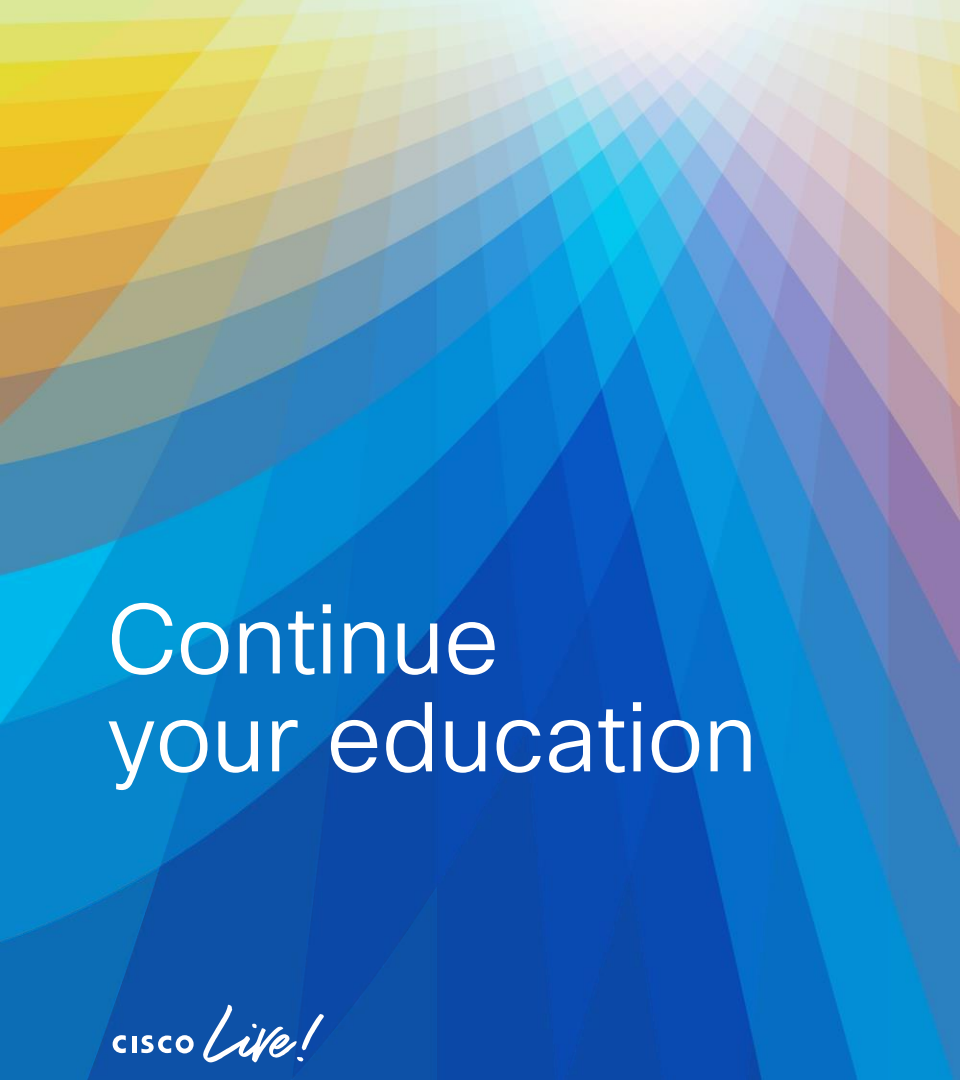
Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!



Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.



These points help you get on the leaderboard and increase your chances of winning daily and grand prizes



Continue your education



- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

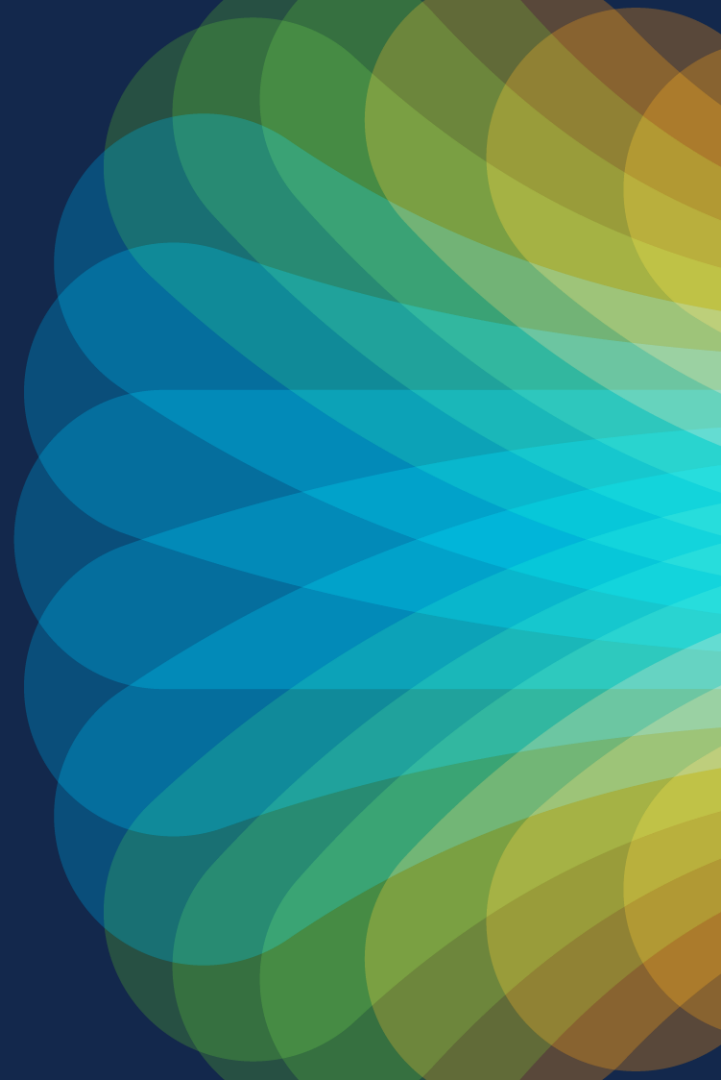


The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive



The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors: yellow, orange, red, pink, purple, blue, and green. Overlaid on this are large, flowing, wavy shapes in shades of orange, red, and yellow, resembling stylized clouds or liquid motion. The overall composition is dynamic and energetic.

cisco *Live!*

Let's go

#CiscoLive